Y4.J89/2:S.HRG.103-1022

S. Hrg. 103–1022

DIGITAL TELEPHONY AND LAW ENFORCEMENT ACCESS TO ADVANCED TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES

JOINT HEARINGS

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

OF THE

SENATE COMMITTEE ON THE JUDICIARY

AND THE

SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS

OF THE

HOUSE COMMITTEE ON THE JUDICIARY

ONE HUNDRED THIRD CONGRESS

SECOND SESSION

ON

H.R. 4922 and S. 2375

BILLS TO AMEND TITLE 18, UNITED STATES CODE, TO MAKE CLEAR A TELECOMMUNICATIONS CARRIER'S DUTY TO COOPERATE IN THE INTERCEPTION OF COMMUNICATIONS FOR LAW ENFORCEMENT PURPOSES, AND FOR OTHER PURPOSES

MARCH 18 AND AUGUST 11, 1994

Serial No. J–103–46

(Senate Committee on the Judiciary)

Serial No. 97

(House Committee on the Judiciary)

Printed for the use of the Senate and House Committees on the Judiciary

GOV'T.
DEPOSITORY
OCT 31 1995
HAMPDEN LAW LIBRARY

SUPERINTENDENT OF DOCUMENTS
DEPOSITORY
NOV 19 2003
BOSTON PUBLIC LIBRARY
GOVERNMENT DOCUMENTS DEPT

U.S. GOVERNMENT PRINTING OFFICE
89–499 CC WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-047613-5

Y 4.J 89/2:S.HRG.103-1022

S. Hrg. 103–1022

DIGITAL TELEPHONY AND LAW ENFORCEMENT ACCESS TO ADVANCED TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES

JOINT HEARINGS

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

OF THE

SENATE COMMITTEE ON THE JUDICIARY

AND THE

SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS

OF THE

HOUSE COMMITTEE ON THE JUDICIARY

ONE HUNDRED THIRD CONGRESS

SECOND SESSION

ON

H.R. 4922 and S. 2375

BILLS TO AMEND TITLE 18, UNITED STATES CODE, TO MAKE CLEAR A TELECOMMUNICATIONS CARRIER'S DUTY TO COOPERATE IN THE INTERCEPTION OF COMMUNICATIONS FOR LAW ENFORCEMENT PURPOSES, AND FOR OTHER PURPOSES

MARCH 18 AND AUGUST 11, 1994

Serial No. J–103–46

(Senate Committee on the Judiciary)

Serial No. 97

(House Committee on the Judiciary)

Printed for the use of the Senate and House Committees on the Judiciary

GOV'T.
DEPOSITORY
OCT 3 1 1995
HAMPDEN LAW LIBRARY

SUPERINTENDENT OF DOCUMENTS
DEPOSITORY
NOV 1 9 2003
BOSTON PUBLIC LIBRARY
GOVERNMENT DOCUMENTS DEPT

U.S. GOVERNMENT PRINTING OFFICE
89–499 CC WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-047613-5

SENATE COMMITTEE ON THE JUDICIARY

JOSEPH R. BIDEN, Jr., Delaware, *Chairman*

EDWARD M. KENNEDY, Massachusetts
HOWARD M. METZENBAUM, Ohio
DENNIS DeCONCINI, Arizona
PATRICK J. LEAHY, Vermont
HOWELL HEFLIN, Alabama
PAUL SIMON, Illinois
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
CAROL MOSELEY-BRAUN, Illinois

ORRIN G. HATCH, Utah
STROM THURMOND, South Carolina
ALAN K. SIMPSON, Wyoming
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
HANK BROWN, Colorado
WILLIAM S. COHEN, Maine
LARRY PRESSLER, South Dakota

Cynthia C. Hogan, *Chief Counsel*
Catherine M. Russell, *Staff Director*
Mark R. Disler, *Minority Staff Director*
Sharon Prost, *Minority Chief Counsel*

Subcommittee on Technology and the Law

PATRICK J. LEAHY, Vermont, *Chairman*

HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California

ARLEN SPECTER, Pennsylvania
LARRY PRESSLER, South Dakota

Bruce Cohen, *Chief Counsel*
Richard Hertling, *Minority Chief Counsel*

HOUSE COMMITTEE ON THE JUDICIARY

JACK BROOKS, Texas, *Chairman*

DON EDWARDS, California
JOHN CONYERS, Jr., Michigan
ROMANO L. MAZZOLI, Kentucky
WILLIAM J. HUGHES, New Jersey
MIKE SYNAR, Oklahoma
PATRICIA SCHROEDER, Colorado
DAN GLICKMAN, Kansas
BARNEY FRANK, Massachusetts
CHARLES E. SCHUMER, New York
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JOHN BRYANT, Texas
GEORGE E. SANGMEISTER, Illinois
CRAIG A. WASHINGTON, Texas
JOHN F. REED, Rhode Island
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
DAVID MANN, Ohio
MELVIN L. WATT, North Carolina
XAVIER BECERRA, California

HAMILTON FISH, Jr., New York
CARLOS J. MOORHEAD, California
HENRY J. HYDE, Illinois
F. JAMES SENSENBRENNER, Jr., Wisconsin
BILL McCOLLUM, Florida
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR S. SMITH, Texas
STEVEN SCHIFF, New Mexico
JIM RAMSTAD, Minnesota
ELTON GALLEGLY, California
CHARLES T. CANADY, Florida
BOB INGLIS, South Carolina
BOB GOODLATTE, Virginia

Jonathan R. Yarowsky, *General Counsel*
Robert A. Lembo, *Counsel/Administrator*
Alan F. Coffey, Jr., *Chief Counsel*

Subcommittee on Civil and Constitutional Rights

DON EDWARDS, California, *Chairman*

PATRICIA SCHROEDER, Colorado
BARNEY FRANK, Massachusetts
CRAIG A. WASHINGTON, Texas
JERROLD NADLER, New York

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
CHARLES T. CANADY, Florida

Catherine LeRoy, *Counsel*
Ivy Davis-Fox, *Assistant Counsel*
James X. Dempsey, *Assistant Counsel*
Virginia Sloan, *Assistant Counsel*
Melody Barnes, *Assistant Counsel*
Kathryn Hazeem, *Minority Counsel*

CONTENTS

STATEMENTS OF SENATE COMMITTEE MEMBERS

Page
Leahy, Hon. Patrick J., U.S. Senator from the State of Vermont 1, 3, 108, 110
Specter, Hon. Arlen, U.S. Senator from the State of Pennsylvania 46
DeConcini, Hon. Dennis, U.S. Senator from the State of Arizona 51
Pressler, Hon. Larry, U.S. Senator from the State of South Dakota 201

STATEMENTS OF HOUSE COMMITTEE MEMBERS

Edwards, Hon. Don, Representative in Congress from the State of California ..4, 107
Hyde, Hon. Henry J., Representative in Congress from the State of Illinois 4
Canady, Hon. Charles T., Representative in Congress from the State of Florida 5, 112
Glickman, Hon. Dan, Representative in Congress from the State of Kansas 52
Coble, Hon. Howard, Representative in Congress from the State of North Carolina 111

CHRONOLOGICAL LIST OF WITNESSES

FRIDAY, MARCH 18, 1994

Louis J. Freeh, Director, Federal Bureau of Investigation 5
Panel consisting of Roy Neel, president, U.S. Telephone Association; and Jerry Berman, executive director, Electronic Frontier Foundation, on behalf of the Digital Privacy and Security Working Group, accompanied by Ronald L. Plesser, Piper & Marbury 53
William C. O'Malley, district attorney for Plymouth County, MA, and president, National District Attorneys Association 97

THURSDAY, AUGUST 11, 1994

Louis J. Freeh, Director, Federal Bureau of Investigation 112
Hazel Edwards, Director, Information Resources Management/General Government, General Accounting Office 126
Roy Neel, president, U.S. Telephone Association 132
Thomas E. Wheeler, president, Cellular Telecommunications Industry Association 148
Jerry Berman, executive director, Electronic Frontier Foundation 157

ALPHABETICAL LIST AND MATERIAL SUBMITTED

Berman, Jerry:
  Testimony 65, 157
  Prepared statement 66, 159
  Letter to:
    Senator Leahy and Representative Edwards from the Electronic Frontier Foundation, Inc., Aug. 11, 1994 163
      Expanded protection for online transactional information 166
    Representative Don Edwards from John D. Podesta, chair, Privacy and Technology Task Force, May 29, 1991 179
  Final Report to Senator Leahy from the Privacy and Technology Task Force 179
Edwards, Hazel E.:
  Testimony 126

Page
Edwards, Hazel E.—Continued
  Prepared statement 128
    Attachment: List of organizations contacted by GAO 130
Freeh, Louis J.:
  Testimony 5, 112
  Prepared statement 14, 114
  Letter to Senator Leahy from Louis J. Freeh, May 10, 1994 36
  Response to questions submitted by Senator:
    Pressler 36
    Leahy 41
  Letters from Digital Privacy and Security Working Group to:
    Louis J. Freeh, Mar. 11, 1994 117
    William J. Clinton, President of the United States and Al Gore, Vice President of the United States, Mar. 9, 1994 119
  Letter to Louis J. Freeh from Senator Leahy and Representative Edwards, Apr. 11, 1994 120
    Technology-based problems encountered by Federal, State, and local law enforcement agencies 121
  Letter to Representative Edwards from:
    Samuel F. Shawhan, vice president, GTE Corp., Apr. 5, 1994 122
    John E. Collingwood, inspector, Office of Public and Congressional Affairs, Apr. 7, 1994 122
  Responses to questions submitted by Representative Edwards 122
Leahy, Hon. Patrick J.:
  Testimony 1, 108
  Prepared statement 3, 110
  Letter to Mr. Charles A. Bowsher, Comptroller General, General Accounting Office, Mar. 24, 1994 131
  Letters to:
    Representative Don Edwards from Charles "Bud" Meeks, executive director, National Sheriff's Association, Mar. 15, 1994 102
      National Sheriff's Association adopted resolution, June 23, 1993 . 103
    Senator Leahy from Victor Oboyski, national president, Federal Law Enforcement Officers Association, Mar. 17, 1994 104
Neel, Roy:
  Testimony 53, 132
  Prepared statement 56, 134
  Letter to Senator Leahy, Apr. 27, 1994 61
  Responses to questions submitted by Senator Leahy 61
  Interim report of the Digital Privacy and Security Working Group 70
Plesser, Ronald L.: Testimony 80, 201
O'Malley, Hon. William C.:
  Testimony 97
  Prepared statement 104
Wheeler, Thomas E.:
  Testimony 148
  Prepared statement 149

APPENDIX

ADDITIONAL SUBMISSIONS FOR THE RECORD

Letter to:
  The U.S. President from the Computer Specialist for Social Responsibility, Jan. 24, 1994 205
  Senator Leahy from Matt L. Rodriguez, superintendent of police, Chicago Police Department, Mar. 17, 1994 207
Letter to Representative Edwards from:
  Chief Sylvester Daughtry, Jr., president, International Association of Chiefs of Police, Mar. 17, 1994 208
  John N. Rose, executive vice president, OPASTCO, Sept. 22, 1994 209
Letter to Senator Leahy and Representative Edwards from:
  Hubert H. Humphrey III, president, National Association of Attorneys General, Mar. 17, 1994 210
  Marc Rotenberg, director, and David Sobel, legal counsel, Computer Specialist for Social Responsibility, Mar. 18, 1994 211

Page
Letter to Senator Leahy and Representative Edwards from—Continued
  Lynne Abraham, district attorney, District Attorney's Office, Mar. 28, 1994 213
Letter to:
  Mr. Casimir S. Skrzypczak, president, NYNEX Science and Technologies, Inc. from James K. Kallstrom, Special Agent in Charge, Department of Justice, Jan. 5, 1994 214
  James K. Kallstrom, Special Agent in Charge, Department of Justice, from Mr. Casimir S. Skrzypczak, ATIS chairman, Telecommunications Industry Solutions, Mar. 1, 1994 215
  Chairman Edward J. Markey, Committee on Energy and Commerce, House of Representatives, from Ralph V. Carlone, Assistant Comptroller General, General Accounting Office, July 17, 1992 217
Organized crime appendix of The President's Commission on Organized Crime 229
National Association of Attorneys General adopted resolution on telecommunications companies and law enforcement responsibilities, July 8–11, 1992 231
National District Attorneys Association resolution concerning the Digital Telephony and Communications Privacy Improvement Act 231
Analysis of informal survey of technical problems encountered by law enforcement in conducting electronic surveillance 232
Prepared statement of Morton Bromfield on behalf of the American Privacy Foundation 235
  Letter to Morton Bromfield from:
    L. Jeffrey Ross, chief, Office of Enforcement Operations, criminal division 237
    William A. Russell, Jr., director, Office of Congressional and Public Affairs 238
  Letter from Morton Bromfield to FBI Director William S. Sessions 238
Statement of:
  Telecommunications Industry Association 239
  AT&T Corp 240
  MCI Communications Corp 243
  David A. Banisar, Esq., Electronic Privacy Information Center 245
    Electronic Privacy Information Center statistical analysis report 246
Analysis of the FBI Digital Telephony Proposal by the Electronic Frontier Foundation, Sept. 18, 1992 251
Department of Justice, Federal Bureau of Investigation summary 259
  Draft of the Digital Telephony and Communications Privacy Improvement Act of 1994 261
    Section-by-section analysis of the act 270
Law enforcement requirements for the surveillance of electronic communications 279
Glossary 290

DIGITAL TELEPHONY AND LAW ENFORCEMENT ACCESS TO ADVANCED TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES

FRIDAY, MARCH 18, 1994

U.S. SENATE, SUBCOMMITTEE ON TECHNOLOGY AND THE LAW, COMMITTEE ON THE JUDICIARY, JOINTLY WITH HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS, COMMITTEE ON THE JUDICIARY,

Washington, DC.

The subcommittees met, pursuant to notice, at 10:35 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy and Hon. Don Edwards presiding.

Also present: Senators Specter, and Cohen (ex officio), and Representatives Edwards, Hyde, and Canady.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. We can begin. I am going to make a brief opening statement and then yield to Chairman Edwards and then the ranking Republican on this side and then my good friend, Henry Hyde, from Illinois.

I should state before I start, however, that it is a matter of great pride to me to be here with Don Edwards, a man I am going to miss, somebody I have known in all my years in the Senate. He was already a senior member of the Congress when I came here and one person I have worked with very closely on so many issues, far more than I could recount here, in the 20 years I have been here. Mr. Chairman, I am proud that you could join us here, and I am going to miss you when you leave at the end of this year.

Representative EDWARDS. Thank you, Pat.

Senator LEAHY. The fourth amendment strikes a delicate balance that we have always maintained to protect our personal privacy to the greatest extent possible. At the same time, it provides for law enforcement needs. This balance is what we, Judge Freeh and others, are here to examine today.

Law enforcement, as we all know, is our way to help secure our personal safety. I do not think there are any times that I can remember when the American people's concern about crime and our vulnerability to crime has been greater than it is today. We have seen the terrorist bombing of the World Trade Center, something that paralyzed not only a great city but, in many ways, much of the rest of the Nation as that situation was sorted out. We have seen the exposure of a foreign spy within the upper echelon of our intelligence agency. We have heard the reports of violent crime in virtually every part of our country, whether it is an urban or rural areas.

Now, I would note for those who are here, these hearings are being chaired by a former State prosecutor and a former FBI agent. I must say that FBI agent has served not only this country but the people of San Jose and the Bay area very, very well, and he will be missed.

What we have to do is to understand where we have come from those days back in 1928 when Justice Brandeis said:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home * * *. Can it be that the Constitution affords no protection against such invasions of individual security?

We have worked in the Congress and in our Federal law enforcement to strike the appropriate balance to protect our individual privacy and expectation of privacy. Ten years ago, in 1984, I asked the then Attorney General whether interceptions of electronic mail and computer-to-computer communications were covered by the Federal wiretap law. The Justice Department's answer 10 years ago highlighted developing communications technology but could not provide a definitive answer. So together with House and Senate colleagues and Federal and State law enforcement, the communications industry and privacy advocates, we worked for the next couple of years, through hearings and legislation proposals, to produce the last major revision of our Nation's wiretap laws, the Electronic Communications Privacy Act of 1986—something I was very proud to work on.

Now, current law requires telephone companies and other providers of electronic and wire services to give all assistance necessary so that law enforcement agents can implement lawful wiretap orders. I think the question we are going to have, the basic question that will be asked a dozen different ways, is why the authority that we enacted in 1986 is no longer sufficient. We need to reassure the public how they will be affected. We have to clarify for telecommunications service providers what duties they are going to be assigned. Finally, we need to consider the ultimate costs of the changes being proposed, but we also have to consider the costs that might be there if we do nothing.

Some suggest that the costs if we go forward will include expenditures of hundreds of millions, if not billions of dollars. But I think more important is the issue of whether we are making merely a course correction or embarking on a fundamental change that will affect how we do business, how innovative technology develops, and how much personal privacy we are able to maintain in a digital, high-tech world.

I hope that we can serve legitimate law enforcement needs without jeopardizing privacy rights or frustrating innovation and the development of new technologies or undercutting the competitiveness of America's high-tech industries. We have maintained a delicate balance for 200 years, but what we are going to do here will actually set much of what we may do as we go into the next century.

[The prepared statement of Senator Leahy follows:]

PREPARED STATEMENT OF SENATOR PATRICK J. LEAHY

The Fourth Amendment to our Constitution provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Within these words and evident in the very structure of the Fourth Amendment is the delicate balance we have always maintained to protect our personal privacy to the greatest extent possible while providing for legitimate law enforcement needs. This is the delicate balance that we are here to examine, again, today.

Law enforcement is, at its core, our way to help secure our personal safety. Never have the American people's concern about crime and our feeling of vulnerability to crime been greater than it is today. We have recently experienced the terrorist bombing of the World Trade Center, the exposure of a foreign spy within the upper echelon of our intelligence agency, and the incessant reports of violent crime in virtually every town, city and rural area in every state in the country.

I observe that these Joint Hearings of the House and Senate are being jointly chaired by a former state's prosecutor and a former FBI agent. I am delighted to share the responsibility for chairing these hearings with the distinguished and longstanding Chairman of the Subcommittee on Civil and Constitutional Rights of the House Judiciary Committee. Don Edwards has announced that after serving 32 years he will not be seeking re-election. His judgment, legislative skills and commitment to serving not only the people of San Jose and the Bay Area in California but the interests of all people and the Nation, will be sorely missed.

When the issue of wiretapping first came before the United States Supreme Court in 1928, Justice Brandeis cautioned:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home * * *. Can it be that the Constitution affords no protection against such invasions of individual security?

The answer to his question is, of course, that the Constitution is our protection from unreasonable searches and seizures, but the technological capabilities Brandeis foresaw are fast upon us.

In 1968 Congress first considered and passed comprehensive wiretap legislation and drew the delicate balance between personal privacy and law enforcement needs.

Ten years ago, in 1984 I asked the then Attorney General whether interceptions of electronic mail and computer-to-computer communications were covered by the Federal wiretap law. The Justice Department's answer highlighted developing communications technology but could not provide a definitive answer. Together with House and Senate colleagues, Federal and State law enforcement, the communications industry and privacy advocates we worked for the next two years, through hearings and legislative proposals, to produce the last major revision of our Nation's wiretap laws, the Electronic Communications Privacy Act of 1986. At the time, we amended the law to take into account developments in communications and computer technology and the structure of the telecommunications industry.

In late February of this year, Director Freeh came to me and other members of Congress to consult about a proposal to revise our wiretaps laws anew in the face of the increasing pace of advances in telecommunications technology and impediments to execution of court-ordered wiretaps. I have great respect for Director Freeh and take very seriously his request that we examine these important issues, as this prompt joint hearing demonstrates. I look forward to hearing from Director Freeh and working with him and other representatives of law enforcement.

Current law requires telephone companies and other providers of electronic and wire services to give all assistance necessary so that law enforcement agents can implement lawful wiretap orders. We need to know why and how that authority is no longer sufficient. We need to reassure the public how they will be affected and clarify for telecommunications service providers what duties they will be assigned Finally, we will need to consider the ultimate costs of the changes being proposed and the risks of inaction. Some suggest float those costs will include expenditures of hundreds of millions if not billions of dollars But more important is whether we are making merely a course correction or embarking on a fundamental change that will affect how we do business, how innovative technology develops and how much personal privacy we are able to maintain in a digital, high-technology world.

My hope is that we can serve legitimate law enforcement needs without jeopardizing privacy rights or frustrating innovation and the development of new technologies or undercutting the competitiveness of America's high-tech industries. Americans' basic values demand that we maintain the delicate balance that has served us so well for over 200 years.

Senator LEAHY. Chairman Edwards?

STATEMENT OF HON. DON EDWARDS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Representative EDWARDS. Thank you very much, Mr. Chairman, and thank you very much for your gracious introduction and welcome. And also thanks for letting Mr. Hyde and me have a visa to come into this grand place.

Mr. Chairman, I think you expressed very well our concerns about the bill and certainly our intention of being responsible in resolving the problem, taking into consideration the very important points that you outlined.

When I was an FBI agent—it was before some of you were born—Mr. Hoover was the boss, and it was illegal for us to tap telephones. I seem to remember we did it anyway, but I do not——

[Laughter.]

Senator LEAHY. I always wondered about that.

Representative EDWARDS. But I will not admit it.

Then in 1968, for the first time, we made wiretapping legal with the certain safeguards. It has been legal ever since. We are anxious to help in the important work that the FBI does. This is an unsafe world, and the work that the FBI does is so important and especially under our new Director, whom we are delighted to have with us today.

Thank you again.

Senator LEAHY. Thank you.

Mr. Hyde?

STATEMENT OF HON. HENRY J. HYDE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Representative HYDE. Well, very briefly, Mr. Chairman, it is an honor to share a podium with Senator Leahy and Don Edwards. Don will be missed. Don is a living example of why term limits are not the brightest idea that I have ever heard.

In any event, I think all of us are working toward the same goal. We want to make sure that the technological advances in the field of telecommunications, which are considerable and ongoing and enormous, will not foreclose the ability of the FBI and other law enforcement agencies to conduct legal electronic surveillance.

Legislation is clearly necessary to help accomplish this goal, and I am confident that both the Senate and the House will work together to carefully craft legislation that will ensure that the delicate balance between citizens' rights of privacy and the important interests of law enforcement are balanced and met.

So I thank you, and I appreciate the opportunity of being here.

Representative EDWARDS. The gentleman from Florida is a new member. We are delighted to have him.

Senator LEAHY. Mr. Canady?

STATEMENT OF HON. CHARLES T. CANADY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Representative CANADY. Thank you, Mr. Chairman.

I want to express my appreciation to both chairmen for conducting this hearing on a subject which is of such great importance to the law enforcement community throughout the United States. The ability of law enforcement authorities to monitor telephone communications pursuant to legal authorization is critical to our crime-fighting and crime-preventing efforts, both at the Federal level and at the State and local level.

The impact that changing technology will have on that ability cannot be ignored. We in the Congress have an important responsibility to listen to the concerns of law enforcement on this important issue and to work with them and the telecommunications industry to fashion workable solutions to the problems and challenges created by the development and expansion of new telecommunications technologies.

I believe that we must do so in an expeditious manner to ensure that we avoid the degradation of law enforcement capabilities and that we also avoid the unnecessary expenditure of funds that may be necessary to correct problems that could have been avoided by timely action.

Thank you.

Senator LEAHY. Thank you.

We are delighted to have Judge Freeh, the Director of the FBI, here. Judge Freeh has received the strong and I think well-deserved support of everybody, certainly on the Senate Judiciary Committee, and I expect the same on the House Judiciary Committee, Republican and Democrat alike.

As I said during the hearings on his confirmation, I feel having somebody with a strong law enforcement background as FBI Director is extremely important.

Incidentally, Judge, I am glad to hear what you told me earlier this morning, that the two agents who were wounded are coming along well. I think the fact that they, like so many others in law enforcement, do face situations like that is a constant reminder that we are not dealing in the abstract in issues of law enforcement. You constantly have a lot of men and women who put their lives on the line, just as State and local law enforcement officers do.

We are delighted to have you here, and your full statement, of course, will be part of the record. Please proceed.

STATEMENT OF LOUIS J. FREEH, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. FREEH. Thank you very much, and good morning to both chairmen and the other distinguished members. It is a delight to be before your distinguished respective committees and to be before you this morning.

The United States is facing a grave and growing problem. New telecommunications technology is impeding or preventing law enforcement from conducting court-authorized electronic surveillance, or what we call wiretapping. The problems are just beginning, in my view.

Congress created a statute 25 years ago that allows wiretapping in the worst and most dangerous cases, cases where no other law enforcement tool can do the job. Throughout that quarter century, wiretapping has been invaluable in protecting our people and safeguarding our national security. But the new technology in the Nation's telephone systems is already thwarting some wiretap efforts. It will be a disaster if this and other emerging telecommunications technologies spread nationwide without needed law enforcement safeguards.

My plea to you today—and it is a plea—is for congressional passage of a statute that would require telecommunications companies to build into that new technology the capabilities that will allow law enforcement to conduct wiretapping with court approval. We are not seeking any expansion of the authority Congress gave to law enforcement when the wiretapping law was enacted 25 years ago. With court approval, law enforcement is now technically able to wiretap on the old technology. We simply seek to ensure a failsafe way for law enforcement to conduct court-authorized wiretapping on the recently deployed and emerging technology. I believe that we are asking for the balance to be maintained instead of being changed.

Unless Congress creates a new law, law enforcement's ability to protect the public against crime will, in my view, be gravely eroded and the national security placed at risk. Wiretapping is used in the most important life-and-death cases: terrorism, espionage, drug trafficking, organized crime, kidnapping, and a variety of other crimes. Without a new statute, law enforcement at the Federal, State, and local levels will be crippled. In all too many instances, an already over-burdened law enforcement system will be fighting with one hand behind its back.

Members of your two distinguished subcommittees surely know as experts that court-approved electronic surveillance is of incredible value, often the only way to prevent or solve the worst crimes. We need to reflect only for a moment for some examples. One deadly terrorist incident has been solved, another terrorist incident prevented, an arrest of an alleged spy in what is surely what is one of the major espionage cases in this or any other decade. Without wiretapping, those important victories for the cause of justice would have never occurred.

If there is no new statute, law enforcement will suffer. The costs to society will be staggering. Crime will claim untold victims who could otherwise have been preserved and protected.

I am an advocate here. I am an advocate for law enforcement, Federal, State, and local; I am an advocate for national security; and I am an advocate for the public safety of the American people.

I am here on behalf of the administration to urge you to solve a major threat to our ability to protect the American public, safeguard the national security, and effectively enforce the law. These new telephone impediments are the unintended side effects of advanced telecommunications technology, which has been and continues to be deployed without consideration for the critical needs of law enforcement.

I am here to assert what the administration and I believe is the only rational and viable means of removing this threat: the enactment of comprehensive legislation to address the digital telephony issue. Without it, one of our most effective weapons against national and international drug trafficking, terrorism, espionage, organized crime, and serious violent crimes will be severely harmed.

The administration wants to work with the Congress to develop such comprehensive legislation, which is why the bill has not yet been introduced. I have shared with each of you a legislative draft for your consideration. The purpose of this legislation, quite simply, is to maintain technological capabilities commensurate with existing statutory authority—that is, to prevent advanced telecommunications technology from repealing, de facto, statutory authority now existing and conferred to us by the Congress.

The proposed legislation explicitly states that it does not alter the Government's authority to conduct court-authorized electronic surveillance and use pen registers or trap and trace devices. The essence of the legislation is to clarify and more fully define the nature and extent of the service provider's assistance requirement that was enacted by the Congress in 1970, which Congress imposed so that court orders would not be frustrated due to a provider's failure to furnish needed technological assistance and facilities. The proposed legislation relates solely to advanced technology, not legal authority or privacy.

We have not sought legislation lightly. For nearly 4 years, we have expended every reasonable effort to address this threat through numerous and ongoing meetings with the telecommunications industry. However, it is my judgment and that of the administration that dialog alone, no matter how well intended, will not solve this serious threat to public safety.

We have listened and learned, and the draft legislative proposal before you represents the only proper balanced approach. It deals with the advanced telephony problem in an appropriately comprehensive fashion. It does not simply "band-aid over" past problems. It also responsibly deals with new services and technologies, such as personal communications systems. On the other hand, the legislation is narrowly focused on where the vast majority of our problems exist: the networks of common carriers, a segment of the industry which historically has been subject to regulation.

The administration's draft proposal approaches the problem in a very rational fashion. It included clearly stated electronic surveillance requirements, systems security provisions, a reasonable deadline for compliance, requirements for equipment manufacturer and support service provider cooperation, proper enforcement and penalty provisions, ongoing government consultation to facilitate compliance, and, importantly, a commitment by the Federal Government to pay common carriers for reasonable charges associated with achieving compliance.

To appreciate fully the need for legislation, it is essential, in my view, that Congress understand the critical importance of electronic surveillance and the severe harm that will result if this critical tool is lost or diminished.

The Nation's phone networks are routinely used in the commission of serious criminal activities, including terrorism and espionage. Organized crime groups and drug-trafficking organizations also rely heavily upon telecommunications to execute their crimes and hide their illegal profits.

In 1968, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968, title III of which contained comprehensive Federal legislation regarding electronic surveillance. Title III established strict procedures for conducting electronic surveillance, procedures that are carefully adhered to by law enforcement and rigorously enforced by the courts. Thirty-seven States also have electronic surveillance laws.

In 1992, a total of 919 title III orders, as well as an estimated 9,000 pen register orders, were authorized for all Federal, State, and local law enforcement agencies. Of that total, only 340 were procured by the Federal Government, of which only 252 were applied for by the FBI. Approximately two-thirds of the criminal-related electronic surveillance conducted in the United States is carried out by State and local law enforcement agencies. As you are aware, title III permits electronic surveillance only for serious felony offenses and only when all other investigative techniques will not work or are too dangerous.

Electronic surveillance is one of the most important investigative techniques, if not the most important, for many cases. Frequently, criminality under investigation could never be detected, adequately investigated, or successfully prosecuted without this critical tool. Though used sparingly, electronic surveillance has been extremely effective, leading to the convictions of thousands of dangerous criminals involved in drug trafficking, organized crime, violent crime, kidnaping, crimes against children, and public corruption. Its evidence has secured the convictions of more than 22,000 dangerous felons over the past decade.

Aside from its great importance as an investigative tool, electronic surveillance frequently has been essential in preventing crimes and saving human life, such as preventing murders, saving numerous lives threatened by terrorist attacks, dismantling organized crime groups which prey on people through extortion and violence, and in attacking the national and international drug cartels whose illegal drugs so ravage society and cause incalculable personal injury.

Although I cannot discuss the details, I can assure you that court-authorized electronic surveillance has played a critical role in successfully resolving two recent highly publicized cases concerning terrorism and espionage. Electronic surveillance has been critical in numerous other cases.

A brief example, the violent El Rukn gang in Chicago, acting as a surrogate for the Libyan Government and, in support of terrorism, planning to shoot down a commercial airliner within the United States using a stolen military weapon. This act of terrorism was prevented directly through the use of electronic surveillance.

The Ill Wind public corruption and Defense Department fraud investigation relied heavily on court-ordered electronic surveillance. To date, this investigation has resulted in the conviction of 65 individuals and more than a quarter of a billion dollars in fines, restitutions, and recoveries. Numerous——

Senator LEAHY. But, Director, if I might, I do not think any of us disagree on the need for electronic surveillance in some of the cases that have been made as a result of it, many of which are ongoing now. I would expect that in your Agency and in State and local agencies, there are a very large number of court-ordered electronic surveillances going on in this country today. But we have in the current statutes involving wiretaps, pen registers, trap and trace devices and so on, required the service providers to furnish forthwith all information facilities, technical assistance and so on necessary to accomplish execution of an order. We all know the technology is changing very rapidly.

What I am concerned about is, why is current law inadequate? If they are required to furnish forthwith everything you need, why isn't that enough?

Representative EDWARDS. Would you yield at that moment, Senator?

Senator LEAHY. Sure.

Representative EDWARDS. They are going to testify that this added legislation is not needed, that they take care of you currently and can take care of you down the road.

Mr. FREEH. Well, I will answer both questions. With respect to the need, the need arises precisely because the companies in 4 years of negotiations have told us and have told me personally in the several meetings I have had with them that, come the changing to the digital switching system and come the changing technology within a very, very short period of time, they will not be able to provide the access that we now get. If there is no problem, then there is no reason for legislation. But they have been telling us that there is a serious problem, and they have been forecasting that within a very short period of time they will not be able to service our court orders.

Their lawyers have advised them that the statute, as currently written, will not obligate them to provide the current access. We are talking also not about one single provider where we could bring a declaratory judgment action in some court and get a ruling. We are talking about 2,000 companies, which, even if we reached a memorandum of understanding with each one, we would never cover the field.

They have told us in discussions over 4 years that we ought to level the playing field, and some have suggested that we do it by statute.

Senator LEAHY. But I am not sure how their lawyers reached this interpretation. How do you interpret it? The statute says that they are required to give all necessary assistance. In fact, there have been some instances where law enforcement agencies have actually gone to court to force telephone companies to provide certain assistance, such as a leased line, remote location monitoring and so on. The courts have always sided with law enforcement. I do not know of a single case where they have not.

How do you read that law? We will ask the telephone companies what their lawyers think, but how do you read current law? Isn't it broad enough to say all necessary assistance means just that?

Mr. FREEH. I do not believe it is, Senator, and if I were an article III judge still sitting in New York—where my Dad said I should have stayed, by the way—I would have great problems compelling the phone company, because it would be by compulsion, to provide something which they do not have and are not currently planning to have on the basis of that language.

There is a great and honored principle in the common law that you cannot compel someone to perform an act that they are incapable of. What they are telling us is they will not have in the switches the software necessary to make the connections to give us the access. I do not think any article III judge facing an appeal to another court would be valid in compelling them to do something which they tell us technologically they cannot do.

Senator LEAHY. So what you are trying to get is to expand current law to make sure they are required to have certain types of equipment that the Department of Justice will tell them to have?

Mr. FREEH. We are not asking them to expand the authority that we have to do wiretapping. I think that has to be clear because there is a lot of misinformation about that.

What we are saying is that we have certain requirements with respect to access which they tell us are not going in the software, and we want to present those requirements to them, and the statute will compel all of the competitors in this field—and there are over 1,500 of them—to put those requirements into their systems as they build the software.

We are just talking about a feature package here. We are not talking about some——

Senator LEAHY. For example, have you had any instances where you have had a court order for a wiretap that could not be executed because of digital telephony?

Mr. FREEH. We have had problems just short of that, and I was going to continue with my statement, but I will not now because I would actually rather answer questions than read.

We have instances of 91 cases; this was based on a 1993 informal survey which the FBI did with respect to State and local law enforcement authorities. I can break that down for you.

Senator LEAHY. In fact, you did provide a breakdown. In your statement, you said, of those 91 wiretap orders, in 10 instances the cellular provider did not have enough capacity, in 19 instances special calling features were the problem, in 30 instances the cellular provider could not give you dialed-number information.

Let's look at the special calling features. Apparently, call forwarding is a problem. With the law that you and the administration are suggesting, would call forwarding be kept off the market unless the companies were able to provide a way for law enforcement to tap into it?

This is a service that tens of millions of consumers who are law-abiding people, have and use. Would that service have had to be kept off the market if they could not find a way to tap it?

Mr. FREEH. Absolutely not, and that is not the intent of the legislation, and I do not believe that that is the effect.

What this heralds, the 29 problems with respect to the calling feature impediments—and it is not all call forwarding—means that as the switches go digital, particularly the central office switches, there will be an increasing number of lapses in the system where we cannot get the access in the normal fashion.

We are not looking to introduce any feature package that impedes technology. And, interestingly enough, last Friday I sat in my building with 38 representatives of the industry, telecommunications companies, and we asked them. We said give us one example of a technological advancement or improvement which you believe this feature package would inhibit. And there was complete silence in the room.

Senator LEAHY. I might suggest one: A private company that wants to build a computer, fax machine, telephone or whatever that is encrypted.

Mr. FREEH. Well, but that is a different problem. We are never asking the phone companies and this legislation does not ask them to decrypt. It just tells them to give us the bits as they have them. If they are decrypted, that is my problem. But that is not going to be addressed in the legislation.

Senator LEAHY. That is going to be another hearing.

Mr. FREEH. I am looking forward to that one, too.

Senator LEAHY. I feel very fortunate to have had all these things land in my subcommittee. Otherwise, I probably would have had nothing to do on weekends and evenings. [Laughter.]

You either. But you talked about 10 instances in your statement where interception orders for cellular phones could not be executed because the provider has insufficient capacity.

Mr. FREEH. That is not a digital problem. That is a capacity problem.

Senator LEAHY. That was primarily in New York City, wasn't it?

Mr. FREEH. It was primarily in New York City, although in the Southern District of Florida, speaking to my counterparts in the DEA, they have documented instances, numerous instances, where they cannot execute title III court orders because of the lack of the access requirements in the company.

Senator LEAHY. We have the problem with cellular phones and other technologies that came on the market so fast and so much quicker than anybody thought. That is part of it, is it not?

Mr. FREEH. That is exactly part of it, and that is why we are here today, because the technology is running at such a pace that we could be out of the wiretap business in a very short period of time. We are already suffering instances of impediments which are preventing the enforcement of court orders.

Senator LEAHY. But we may end up also holding back technology to preserve wiretaps. We are talking about the Federal Government paying for some of the various costs. You have one provision in your proposal to require telephone companies to designate personnel to be on call 24 hours a day to activate the Government's intercept orders. Are we going to pay for that on-call person? If you are dealing with the local telephone companies, say here in Washington or in New York City, that does not seem like a big problem. Are we going to pay for them?

Mr. FREEH. I think we do pay for that, but I do not think those costs are excessive at all. If you are talking about 919 wiretaps in the whole United States by every Federal, State, and local authority, that is a very small number of wiretaps, which is precisely why the access is so critical, because we select out only the most important dangerous cases to use the technique for.

Senator LEAHY. So if the Topsham Telephone Co. in Topsham, VT, which has five employees, is concerned, we could tell them that if they have got to have somebody on call there, you guys would pay for it?

Mr. FREEH. I think if they have the right software package that they could probably design much cheaper than the Federal Government. They could be home sleeping at night, and we could still get the access we need.

Senator LEAHY. Let me go back to something you said earlier. You said technology may be fast outstripping the capacity to wiretap. By the same token, what that means is that if this legislation were passed, you would be able to, in effect, stop all this technological advancement until it was redesigned in such a way that you could tap. Is that correct?

Mr. FREEH. I do not think that is correct, respectfully. Again, I am basing this not on my own engineering skills, of which I have none, but on the report of the working group, the industry and law enforcement working group that has discussed this issue for 4 years. The group, the industry group, by the way, is the entity that identified this as a grave problem that has to be solved and has to be addressed. It is not the FBI coming in and saying we have the problem. it is the phone companies telling us they are not going to be able to serve our orders.

In terms of the technology, I do not think we impede technology. I think that——

Senator LEAHY. Well, we may be talking past each other on this. The phone companies obviously are moving forward on technology. It is moving very rapidly. They have come to you and said that this is technology you probably will not be able to tap into, and I share your level of engineering experience. I suspect yours is higher than mine. But let us just take the facts as they state them.

Mr. FREEH. All right.

Senator LEAHY. They are moving forward to develop new technologies. They have told you this technology is something you cannot tap into. It is obviously technology they feel they want, or they would not be moving forward on it. We are talking about hundreds of millions, even billions of dollars of investment on their part. You are saying, wait a minute, we have to be able to tap into this, and we are going to go to the Congress, and get legislation to tap into it. Well, then, doesn't it follow that that technology has either got to change, stop, wait, or develop some new feature to work, and it is not going to be the technology that they have made the corporate decision to go forward with?

Mr. FREEH. Well, again, I respectfully disagree. I think if the phone company—we have met with engineers, and I do not have an engineering background, but at the meeting last Friday the GTE representative told us that they are now building switches. They are building switches which will be marketed 2 or 3 years from now. What he said is, look, give me the requirements—the industry has to know what the requirements are—and we will build those into the switches, in effect. Not that they want to do it and not that they would rather do something else, but they are not telling us that this is an impossibility.

Senator LEAHY. Your response to that is give us technology that we can tap, but you do not need a new law for that.

Mr. FREEH. We do because they will not do it voluntarily. Two thousand companies will not sit down at the same table and agree unilaterally to do exactly the same thing with respect to our requirements.

Senator LEAHY. So what you are saying is that you want this committee to set an industry-wide uniform standard, which may not be the standard the industry wants and may be legislatively impeding technological advances that would be there without our stepping in.

Mr. FREEH. Yes, yes, we want this committee to set and mandate requirements in future equipment which is currently being engineered and deployed to give us the continued access, the access which the Congress gave us in 1968. And I will wage if you ask the American people whether they would want a feature package on their phones where we can find their children when they are abducted, they would say fine, we would like that feature. That is a real nice feature to have on our telephones. That is what we are asking for.

Senator LEAHY. What if we told them we have some major technological advances coming that would make life easier but we are going to hold it up? We are also going to add significant costs both through taxes and service fees to do this.

Mr. FREEH. Well, it is a cost-benefit analysis. I sat last week with Polly Klaas' father, who came in from California to talk to me, and he said to me, "Mr. Freeh, the FBI did everything in that case to find my little girl." I do not want to be in the position where I am going to tell some father that I could not do everything I would normally do because I could not get the access that I have today.

Senator LEAHY. Mr. Edwards?

Representative EDWARDS. Thank you, Mr. Chairman.

Other countries, modern countries like the United States, must be having the same problem because they do the same kind of work that the FBI does in wiretapping. Is this true? Are you in communication with Germany and Britain and the other friendly nations?

Mr. FREEH. Yes, Mr. Chairman, we are. In fact, Jim Kallstrom just came back from England where he met with people in the police as well as the home secretary. I met with the German Minister of the Interior back in December. They are doing exactly what we are doing, and they are going to follow our lead since we are the leader in telecommunications.

What they have told us is that they would like to take our industry standards and put them into their telecommunications carriers, which means that instead of being noncompetitive, American companies who build these features in will actually be more competitive overseas because our counterparts want the exact same access that we are going to need in the new technology.

Representative EDWARDS. Are you serious about a $10,000 a day fine of companies that are recalcitrant?

Mr. FREEH. I think that is flexible. I think for the most part an article III judge has, under the All Writs Act, powers well beyond $10,000 fines and injunctions. The reason we put that into the proposal is that it gives a benchmark; it also gives some guidance to the district courts as to the area where they should operate. But I do not think that is a necessary authorization. I think any title III judge has that power now. We do not use it because the phone companies have been very, very cooperative with us.

Representative EDWARDS. My last question, Director Freeh. How much is this going to cost the Government?

Mr. FREEH. We estimate $300 to $500 million. That could be off by $200 million. It could be off by $500 million. There is no good rock-bottom answer in terms of the money.

I do not think it is going to cost more than a billion dollars. The industry in our meeting last week is not sure either. Someone said it would be a minuscule cost. Someone else said it would be a couple of billion dollars.

What I do know is that the World Trade Center cost us $5 billion in damages when it was blown up and that these costs, like the 911 system, are really, on a cost-benefit analysis, worthy of people's investment.

[Mr. Freeh submitted the following:]

PREPARED STATEMENT OF LOUIS J. FREEH, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

SUMMARY

In summary, it is my view that the digital telephony issue is the number one law enforcement, public safety, and national security issue facing us today. The maintenance of an effective electronic surveillance capability is essential to our nation's law enforcement and intelligence agencies. This investigative technique is a unique and indispensable weapon against national and international drug-trafficking organizations, organized crime syndicates, terrorist groups, and violent criminal conspiracies. Without an effective electronic surveillance capability, our law enforcement and intelligence agencies will not be able to protect the public adequately or acquire the evidence needed to put some of society's most dangerous felons in jail. Recent efforts to ensure substantial jail time for violent, hardened criminals will be undercut, if we in law enforcement first cannot identify them, arrest them, and obtain the compelling evidence required to secure their convictions.

As you are aware, after an extensive review of this serious problem the administration has concluded that Federal legislation is the only viable means of solving the so-called "digital telephony" problem. The technological impediments to court-ordered electronic surveillance, which are the unintended by-products of advanced digital telephony, constitute a major nationwide obstacle to effective law enforcement. To date, numerous court orders have been frustrated, in whole or in part, by these impediments. Left unaddressed, this problem will soon grow to dangerous proportions. The Federal Bureau of Investigation and the entire Federal, State, and local law enforcement community are completely unified in our assessment that impediments which hinder or preclude court-ordered electronic surveillance must not be allowed to stand.

The decision to press for legislation was not reached lightly. Over the last four years, we have made substantial efforts to resolve this matter through numerous meetings with leaders in the telecommunications industry. Included in these efforts has been a law enforcement/industry technical working group which was specifically instituted by industry to "solve the problem." Even though we have met for nearly two years (and have mutually benefited from the discussions), there is no mechanism for assuring the timely, comprehensive development and implementation of the required technological solutions. In fact, the chairman of the industry technical working group acknowledges this fundamental shortcoming and problem. Obtaining these solutions can no longer be left to chance. Federal legislation represents the only realistic prospect for obtaining, with certainty, the timely and comprehensive development and implementation of the required technological solutions by the telecommunications industry.

As I indicated, the proposed legislation is focused on "mainstream" telecommunications service providers, on "common carriers," who historically have been subject to regulation. This legislative proposal should be more acceptable to the common carriers. For instance, the electronic surveillance requirements have been clarified;

a network "systems security" provision added, which specifies that all premises-based intercepts (switches, network elements) must be activated exclusively by common carrier personnel; a mandate that support service providers and equipment manufacturers, upon whom the carriers rely, will furnish the timely cooperation required to permit compliance; an Attorney General "consultation" provision designed to facilitate discussion and cost-effective approaches to compliance; and, importantly, Federal Government payment to common carriers for reasonable and cost-effective charges directly associated with attaining compliance which are incurred within the three year period set for compliance.

Also included in the legislation are amendments to the Federal criminal electronic surveillance laws ("Title III") which improve communications privacy protection: privacy protection for handheld "cordless" telephones on a par with wireline and cellular telephones, clarification of privacy protection for electronic communications transmitted by radio, and privacy protection for communications transmitted using security-enhancing modulation techniques.

Law enforcement fully supports the introduction and deployment of advanced telecommunications technologies as a means of sharing information, educating Americans, and increasing our productivity. In particular, we are extremely supportive of the Vice President's initiative to create a national information infrastructure for the benefit of all Americans. As we all embrace the vast potential offered by advanced technology, and advanced telecommunications technology in particular, it is critical that the equities of our law enforcement and intelligence agencies not be forgotten or ignored. However, it would be wrong for all of us as public servants, both within the executive and legislative branches of government, to knowingly allow this information superhighway to jeopardize the safety and economic well-being of law-abiding Americans by becoming an expressway and safe haven for terrorists, spies, drug dealers, murderers, and thugs.

I do not relish the thought of being the first FBI Director to tell a father and mother that we were unable to save their son or daughter because advanced telecommunications technology precluded the telephone company from providing us with lawful access to the criminal conversations that would have prevented the untimely death of an innocent child. Nor do I want the president placed in the position of having to tell the American public that we in law enforcement could not prevent a violent terrorist act directed against innocent Americans in a major metropolitan area solely because of advanced telecommunications technology.

It is imperative that Congress promptly enact the administration's proposed legislation that will solve this serious problem on a timely and comprehensive basis. Every day that passes in which this problem remains unresolved, the longer the safety and economic well-being of the American public are unnecessarily placed at risk. I look forward to working with each one of you and this Congress regarding the enactment of this important legislative initiative.

Thank you Mr. Chairmen and the members of these Subcommittees for providing me this opportunity to testify and provide you with information concerning the most important public safety and national security issues facing us today.

Mr. Chairmen, I appreciate the opportunity to appear before your subcommittees. I am here today not just in my capacity as Director of the Federal Bureau of Investigation but also as a spokesman for our nation's law enforcement and intelligence communities regarding a matter of extreme urgency and importance. I am here on behalf of the administration to tell you that we are confronted with a major threat to our ability to protect the American public, safeguard the national security, and effectively enforce the law. This threat results from various technological impediments to our ability to execute court orders and lawfully conduct electronic surveillance and acquire the associated dialing information. These impediments are the unintended side effects of advanced telecommunications technology which has been, and continues to be, deployed without consideration for the critical needs of our nations law enforcement and intelligence agencies.

I am here today to strongly assert what I and the administration believe is the only rational and viable means of removing this threat—the enactment of the proposed comprehensive legislation to address the digital telephony issue. Without its enactment, one of our most effective weapons against national and international drug trafficking, terrorism, espionage, organized crime, and serious violent crimes will be severely and adversely impacted.

The administration wants to work with the Congress to develop such comprehensive legislation. I will describe in this testimony a draft legislative proposal that has been shared with you.

Quite simply, the purpose of this legislation (draft) is to maintain technological capabilities commensurate with existing statutory authority—that is, to prevent advanced telecommunications technology from repealing *de facto* the statutory authority already conferred by the Congress. The proposed legislation explicitly states that the legislation does not enlarge or reduce the government's authority to lawfully conduct court-ordered electronic surveillance and install or use court-ordered pen register or trap and trace devices. The essence of the draft legislation is to clarify and more fully define the nature and extent of the telecommunications service provider's "assistance" requirement that was enacted by Congress in 1970. That requirement evidenced Congress' clear intent that lawful court orders should not be frustrated due to a service provider's failure to provide needed technological assistance and facilities. The proposed legislation relates solely to advanced technology, not legal authority or privacy.

We did not come to seek legislation blithely. For nearly four years, the FBI has expended every reasonable effort to address this threat through numerous and ongoing meetings with the telecommunications industry. However, it is my considered judgment, and that of the administration, that dialog alone, no matter how well intended, will not solve this serious threat to public safety. Nonetheless, we have listened and learned, and the legislative proposal before you represents, in our estimation, the only proper approach. On the one hand, it deals with the advanced telephony problem in an appropriately comprehensive fashion—it does not simply "band-aid-over" past problems, it also responsibly deals with new services and technologies (such as personal communications services) that likely will emerge in the next few years. On the other hand, the draft legislation is narrowly focused and covers on only those segments of the telecommunications industry where the vast majority of the problems exist—that is, on common carriers, a segment of the industry which historically has been subject to regulation. We believe the provisions of the administration's proposal address the problem in a very rational fashion. They include clearly stated law enforcement electronic surveillance requirements, systems security provisions, a reasonable deadline for compliance, requirements for equipment manufacturer and support service provider cooperation, proper enforcement and penalty provisions, ongoing government consultation with common carriers to facilitate compliance, and, importantly, a commitment on the part of the federal government to pay common carriers for reasonable charges associated with achieving compliance.

IMPORTANCE OF ELECTRONIC SURVEILLANCE

As the proposed legislation is considered, it is absolutely essential that Congress understand the importance of electronic surveillance, as well as the severe harm that will occur if this critical law enforcement tool is lost or diminished.

The nation's telecommunications networks are routinely used in the commission of serious criminal activities, including terrorism and espionage. Organized crime groups and drug trafficking organizations, which are often highly structured, rely heavily upon telecommunications to plan and execute their criminal activities and hide their illegal proceeds. Similarly, foreign intelligence service officers and their agents carry out their spy and other clandestine missions through these networks.

Congress recognized this fact a little over 25 years ago, when it passed the Omnibus Crime Control and Safe Streets Act of 1968. Title III of that Act contained the first comprehensive federal legislative regimen regarding electronic surveillance for use in criminal investigations. The Title III legislation established strict procedures for the conduct of electronic surveillance by federal, state and local law enforcement authorities. These procedures are carefully adhered to by law enforcement and are rigorously enforced by the courts. To date, thirty-seven (37) states, Puerto Rico, the U.S. Virgin Islands, and the District of Columbia also have enacted electronic surveillance statutes. In 1992, a total of 919 Title III orders, as well as an estimated 9,000 pen register orders, were authorized for all federal, state, and local law enforcement agencies. On average, approximately two-thirds of the criminal-related electronic surveillance conducted in the United States is carried out by state and local law enforcement agencies. As mandated in the Title III legislation, electronic surveillance may be used only in the investigation of serious felony offenses and only when other investigative techniques will not work or are too dangerous.

In 1978, Congress established an analogous federal electronic surveillance regimen for use in counter-intelligence, counter-terrorism, and counter-espionage investigations, the foreign intelligence surveillance act of 1978 (FISA). Pursuant to FISA, the U.S. Government is authorized to intercept communications of individuals who pose a threat to the national security, and include those in furtherance of espionage and terrorism.

Since the passage of Title III, law enforcement has found electronic surveillance to be one of its most important investigative techniques—if not the most important. Use of the technique has been critical in fighting organized crime, drug trafficking, public corruption, fraud, terrorism, and violent crime, and in saving numerous innocent lives. In many of these cases, the criminal activity under investigation could never have been fully detected, prevented, adequately investigated, or successfully prosecuted without the use of evidence derived from court-ordered electronic surveillance. Similarly, FISA-based intelligence information makes a significant and important contribution to U.S. counter-intelligence, counter-terrorism, and counter-espionage efforts.

As you are aware, electronic surveillance is a critical tool used to detect and obtain evidence of, and often prevent, the most serious, and often most violent, criminal activity confronting our society. As shown in the attached exhibit, although used sparingly, electronic surveillance has proved to be an *extremely* effective investigative technique for law enforcement and has led to the convictions of thousands of dangerous persons involved in drug trafficking, organized crime, violent crime, kidnaping, crimes against children, and public corruption. Because a substantial number of prosecutions are ongoing, the exact number of convictions resulting from these wiretaps increases almost daily; however, this key investigative technique has proven to be incomparably effective, with the resulting evidence securing the conviction of over 22,000 dangerous felons over the past decade.

PUBLIC SAFETY: PREVENTING CRIMES AND SAVING HUMAN LIVES

Although electronic surveillance is extremely important as an investigative tool to acquire evidence, frequently it has been essential in preventing crimes from occurring and in saving human life. Electronic surveillance has been essential in preventing murders; in saving human life put at risk through planned terrorist attacks; in dismantling entrenched organized crime groups which severely harm the economy through extortion, fraud, and corruption; and in attacking the major national and international drug importation and distribution cartels and networks whose activities ravage society and cause incalculable personal and economic injury in the United States.

ORGANIZED CRIME INVESTIGATIONS

The activities of organized crime are extremely harmful to American business and industry, labor unions, and individuals in our society. Electronic surveillance is indispensable in combating organized crime. Indeed, the FBI's organized crime/drugs section reports that *every* major FBI organized crime investigation has relied upon electronic surveillance. In April, 1988, the importance of the electronic surveillance technique was formally recognized in hearing testimony before the U.S. Senate permanent subcommittee on investigations, Governmental Affairs Committee, on Organized Crime: "25 years after Valachi." in particular, David C. Williams, Office of Special Investigations, General Accounting Office, testified that "electronic surveillance is another tool that has been of great value to the law enforcement community to combat the La Cosa Nostra (LCN) (organized crime families). Evidence gathered through electronic surveillance * * * has had a *devastating impact* on organized crime." (emphasis added)

Left unchecked, organized crime exerts a choke hold on society, and the subsequent cost to business and industry is dramatic. Greater detail concerning areas of organized crime's penetration in business and labor unions and examples of the successful use of electronic surveillance to effectively combat the adverse impact of organized crime upon the economy and society is set forth in the attached appendix.

In the 1986 report, *The Impact: Organized Crime Today,* the President's Commission on Organized Crime utilized the Wharton Business School's long-term model of the United States economy to estimate the cost of organized crime on the economy, in terms of sustained higher prices and the continued underpayment of taxes to the Federal Government. The commission concluded that the estimated economy-wide impact of organized crime, excluding drug trafficking organizations, was as follows:

- U.S. output was reduced by $18.2 billion in 1986 dollars.
- U.S. employment was reduced by 414,000 jobs.
- Consumer prices were higher by 0.3 percent; and,
- Per capita personal income was lower by $77.22, measured in 1986 dollars.

FBI organized crime program managers state: *"The loss or impairment of the capability to conduct court-ordered electronic surveillance would catastrophically im-*

pair Federal and State law enforcement agencies' ability to effectively investigate organized criminal groups." (emphasis added)

Although no studies have been conducted to measure the precise economic and societal benefits derived from the successes of Federal and State criminal law enforcement agencies against organized crime, it is evident that an abatement in successful organized crime investigations, due to the loss or impairment of one of law enforcement's most important tools—the court-ordered electronic surveillance technique—would allow organized crime's damage to the U.S. economy to become substantially greater.

NARCOTICS AND DANGEROUS DRUGS

The greatest use of electronic surveillance by law enforcement relates to the federal and state governments' "war on drugs." Information reported in the Federal wiretap report by the Administrative Office of the United States Courts indicates that almost two thirds (62 percent) of all Title III governmental electronic surveillance is devoted to this critical national problem. The major drug trafficking organizations which import and distribute drugs, like any business organization, rely heavily on telecommunications to coordinate and carry out these criminal activities and to "launder" the billions of dollars in illegal drug proceeds. Accordingly, Federal and State law enforcement maximize their limited resources and focus electronic surveillance efforts on the main drug importation and distribution networks.

Although figures abound with regard to the billions of dollars in Federal, State, and local seizures of drugs, illegal drug proceeds (cash and other assets), etc., the fundamental harm to society is incalculable. It is impossible to fully identify the human, economic, and other societal harm brought about by drug dependency and addiction. In one attempt to quantify certain facets of this harm, the U.S. public health service has estimated the health, labor, and crime costs of drug abuse at $58.3 billion in 1988, exclusive of the value of the drugs themselves. D. Rice, et al., U.S. Department of Health and Human Services, *the Economic Cost of Alcohol and Drug Abuse and Mental Illness: 1985*, table 1, page 2 (1990). A 1992 U.S. Department of Health and Human Services' study estimates the 1992 costs of drug abuse in the United States to be $168 billion or $675 per person. Approximately $40 billion a year are spent by users to procure these drugs.

Ultimately, the economic, societal, and personal harm of drug trafficking is also measured in daily "drive-by shootings" in neighborhood streets (where the blood of innocent children is spilled next to that of neighborhood drug lieutenants); substantially increased crime such as thefts, robberies, and murders brought about by drug use; violent "turf battles" to control drug distribution; lost productivity; employee absence; extensive and expensive health care with drug casualties that clog our hospital emergency rooms; as well as the sad occurrence of a generation of drug-dependent babies.

The drugs which are most responsible for this problem are essentially those (such as cocaine and heroin) which must be imported into the United States, generally by highly organized criminal groups, drug trafficking cartels and other syndicates, and thereafter transported over vast distances and distributed widely within the United States. *These cartels and organizations rely heavily on telecommunications to carry out their illegal activities.* The United States Government estimates that *every year* over 400 metric tons of cocaine and approximately 18 to 22 metric tons of heroin are smuggled into the United States.

Electronic surveillance is critical in the monitoring of the drug traffickers' "communications networks," providing law enforcement with the ability to identify all of the organization's drug traffickers and their illegal proceeds, as well as ultimately in dismantling those national and international drug trafficking organizations. Since national and international drug chieftains and local drug "kingpins" do not appear at drug buys or shipments, electronic surveillance ordinarily provides the only reliable method of linking the drug organizations' leaders with the enterprise, and frequently provides the only direct and persuasive evidence that will support a criminal conviction. Consequently, information derived from electronic surveillance is essential in successfully prosecuting those at the executive level of the drug trade.

Recent examples of the critical role of electronic surveillance in drug investigations are:

- In a New York City-based drug trafficking investigation, an FBI-led task force conducted over 55 separate electronic surveillances (with numerous extensions). As of March 1993, this investigation has resulted in 222 arrests; 167 convictions; the dismantling of 15 major drug trafficking organizations/gangs, and the identification of 30 others; the resolution of some 40 New York area homicides, including the assassination of a NYCPD police officer and a New York state pa-role officer. Substantial quantities of drugs have been seized and over $8 million in assets have been seized. These efforts have resulted in a substantial reduction in drug-related homicides;

- The April, 1992, drug raid in Miami that netted 15,000 pounds of cocaine which was based on information developed through electronic surveillance. Evidence derived from electronic surveillance was instrumental in identifying the network's leader among the 22 defendants arrested;
- The 1991 DEA Herrera Drug Investigation in New York City resulting in the successful prosecution of 51 defendants, including key individuals linked to the call drug cartel, relied upon electronic surveillance.

Without the use of one of federal and state law enforcement's most important enforcement tools—electronic surveillance—the volume of drugs would dramatically increase and the ease and means of drug importation and distribution would be dramatically enhanced through the drug traffickers' unfettered use of their drug "communications networks."

PUBLIC CORRUPTION AND GOVERNMENTAL FRAUD

Integrity in government is a keystone in any democracy. Corruption and fraud undermine the public's respect and confidence in governmental institutions and in the rule of law. By their nature, corruption and fraud can only flourish in secrecy, hidden from public view. As a result, normal, overt investigative techniques are in most cases totally unavailing. Hence, as a general proposition, law enforcement has found that electronic surveillance and undercover operations are critical means to effectively detect, investigate, and prosecute these insidious crime problems.

In several recent judicial corruption investigations, electronic surveillance evidence has directly led to the conviction of two federal district court judges and, in another case, to the indictment or plea of six current of former Dade County, Florida, State judges (four convicted, one acquitted, and one to be retried) and five attorneys (all convicted) for extortion and case fixing. Within the recent past, electronic surveillance helped build a corruption case involving the police force of a large midwestern city which included extortion and protection for gambling and narcotics distribution. Thirty police officers and 17 others were indicted, and 46 of the 47 either pled or have been found guilty.

Electronic surveillance has played an indispensable role in countering governmental fraud. For example, the "ill-wind" investigation (which was largely based upon 36 separate court-ordered electronic surveillances conducted across the United States) has had a tremendous impact upon fraud and abuse both within the government and within the industries that contract with the government. To date, the "ill-wind" investigation has resulted in 65 convictions (including high-level Department of Defense officials and eight corporations), sanctions against contractors, and over a quarter of a billion dollars ($271,000,000) in fines, restitutions, and recoveries ordered. *Evidence necessary to obtain these convictions fines recoveries etc., would have been impossible to obtain without electronic surveillance.*

The high cost of health care in the United States is a problem of tremendous importance to our society. Unfortunately, billions of health care dollars are wasted through fraud. With regard to health care fraud, electronic surveillance has been extremely important. In 1993, in New York, electronic surveillance of hardwired (fixed) and cellular (mobile) telephones produced critical evidence in a case involving widespread Medicare/Medicaid fraud carried out by numerous pharmacies and pharmacists. Seventy-nine (79) individuals, including 38 pharmacists, were indicted. To date, 79 individuals have been convicted or pled guilty and $6.6 million in assets are subject to seizure and forfeiture. Similarly, in 1993, in Detroit, electronic surveillance was instrumental in investigating and prosecuting a wide-spread Medicare/Medicaid fraud perpetrated by numerous pharmacies and pharmacists.

Thirty-two (32) pharmacies/pharmacists were prosecuted, and $4 million in criminal forfeitures are expected to follow. The FBI estimates that the health care fraud in of the foregoing cases alone ranged in the tens of millions of dollars.

Recently, a major governmental fraud case involving Russian emigre organized crime and the Gambino LCN organized crime family was successfully investigated through the use of an undercover operation and the substantial use of electronic surveillance to intercept a number of cellular telephones. The criminal scheme involved defrauding the Federal Government and State governments of motor fuel taxes. The Department of Justice estimates than more than $1 billion in federal excise tax, funds that are earned for the highway trust fund for use in maintaining the nation's highway infrastructure, is illegally "skimmed" each year. An indictment in the foregoing case has been returned in Newark, charging 14 individuals with defrauding the Federal Government and the State of New Jersey out of more than

$60 million in tax revenues and with laundering $66.2 million resulting in 4 convictions *to date.* A number of the subjects in this investigation utilized cellular telephones and frequently changed cellular telephones in an effort to thwart electronic surveillance. The intercepted telephone conversations were critical to proving the involvement of the LCN in this Russian organized crime fraud against Federal and State Governments.

TERRORISM

A significant number of terrorist acts, including bombings and murders, have been prevented through the effective use of electronic surveillance. Many of these terrorist acts, if not prevented, likely would have had substantial national and/or international implications. In one case, the bombing of a foreign consulate in the United States was prevented, and the electronic surveillance evidence was used in the subsequent conviction of the principals. In another case, a terrorist rocket attack against a United States ally by a foreign-based terrorist group was thwarted, and the electronic surveillance-based investigation led to the arrest of the principals and the prevention of the loss of life of scores of persons.

In 1986, the efforts of the violent El Rukn Chicago street gang to shoot down a commercial airliner within the United States with a stolen military weapon system was thwarted through electronic surveillance. The FBI's prevention of this act of state-sponsored terrorism, financed by Libya, which would have cost several hundred U.S. lives, was singularly attributable to the use of electronic surveillance—but for the availability of this technique, another pan an 103 disaster could have occurred on American soil.

More recently, in 1993, electronic surveillance contributed to the indictment of individuals in the St. Louis-based cell of the ABU Nidal organization on RICO charges of murder, conspiracy to commit murder, and conspiracy to bomb the Israeli embassy in Washington, DC in 1990, foreign-based terrorists were prevented from acquiring a stinger surface-to-air missile which was to be employed in a terrorist act wherein numerous people would undoubtedly have been killed. Also, in 1989, as a direct result of court-ordered electronic surveillance in a terrorist-related matter, information was obtained which resulted in the conviction of two individuals for the brutal homicide of their 16-year-old daughter.

Beyond the foregoing instances, over the last decade numerous other terrorist-related investigations have utilized electronic surveillance to: prevent a rocket attack against an FBI field office; prevent an attack on a nuclear power facility; solve several murders; identify the perpetrators of a $7,000,000 armed robbery; and solve and prevent several bombings by anti-Castro groups in Miami, Florida.

VIOLENT CRIME

Many violent crimes, including murder, have been solved and a significant number prevented by law enforcement's "real time" response to, and preventive actions taken as a result of conversations intercepted through electronic surveillance. Electronic surveillance has been used in combating and solving violent crimes perpetrated by both organized criminal groups and by individuals. The following are recent examples of cases in which electronic surveillance has been crucial in saving lives or preventing violent acts from occurring:

- Conversations of members of the New England LCN family were intercepted wherein the murders of three individuals were planned, and details concerning six prior murders were discussed. Of the three planned murders, two were prevented by the FBI; the third could not be prevented because of an inability to locate the victim prior to his murder.
- One of the most violent Asian organized crime gangs active in the New York City area is the Green Dragons, which, as of 1990, was directed telephonically by Kin Fei Wong from the People's Republic of China. The Green Dragons Gang perpetrated murder, armed robberies, home invasions, extortion, drug trafficking, and were involved in the obstruction of justice. Court-ordered electronic surveillance provided evidence of these crimes and also disclosed that the Green Dragons were about to engage in a "shoot out" with a rival Asian gang. Immediately acting upon this information, 16 members of the group were arrested by FBI agents and police officers and an imminent violent confrontation and loss of life were prevented. Based partly upon evidence derived from electronic surveillance, all defendants were found guilty of racketeering, racketeering conspiracy, and numerous substantive counts which included murder, kidnapping, home invasions, armed robbery, extortion and bribery of a public official.

- In 1991, the murder of a United States court of appeals judge was solved and a conviction obtained based in part upon electronic surveillance information.
- In a notable 1990 "sexual exploitation" of children case which relied heavily upon electronic surveillance, the FBI thwarted two individuals who were conspiring to abduct, torture, and kill a teenage boy for the purpose of making a "snuff murder" film.
- In 1993, in Greene County, Ohio, a 10-year old triple homicide was finally solved, and evidence critical for successful prosecution was obtained through the use of electronic surveillance. The victims, two men and a pregnant woman, had been shot execution-style, and subsequently their throats had been slit and their skulls had been crushed by the murderers.

FOREIGN COUNTERINTELLIGENCE (FCI)

Because any discussion of the importance of FISA-based electronic surveillance would involve highly sensitive matters and highly classified information, suffice it to say that information derived from FISA electronic surveillance is critical to the president of the United States, the national security council, the intelligence community, the department of defense, and the state department. Such information is of great importance as our nation's leaders establish policy and safeguard the nation's defense and national security.

CONSEQUENCES OF THE LOSS OF ELECTRONIC SURVEILLANCE

As indicated above, society's most dangerous criminal organizations and groups rely heavily upon the use of telecommunications. Additionally, such organizations tend to take advantage of advanced telecommunications and services to conduct and carry out their illegal activities. Evidence is developing that indicates criminal organizations are also increasingly looking for ways to avoid law enforcement's electronic surveillance by frequently changing their telecommunications devices and telephone numbers, modifying and reprogramming their cellular telephone identification numbers and codes, and utilizing call-forwarding features, etc. increased use of cellular telephones, call-forwarding features, and evasive efforts have already had a negative impact upon electronic surveillance and law enforcement's ability to protect the public and effectively enforce the law. The foregoing cases directly demonstrate the public safety and law enforcement benefits directly attributable to the use of electronic surveillance. They also indicate the kind of negative impacts and societal harms that would result if there were a loss or diminishment of the electronic surveillance technique. Indeed, loss of a viable, effective electronic surveillance technique would result in:

- A substantial loss of life, attributable to the inability of law enforcement to prevent planned terrorist acts and murders;
- A substantial increase in economic harm (in the billions of dollars) to business, industry, labor unions, and society generally caused by the growth/emergence of organized crime groups and activities;
- A substantial increase in the corruption of legitimate business, industry, and labor unions caused by the growth/emergence of organized crime groups;
- A substantial increase in the availability and reduced cost of narcotics and illegal drugs, as well as the attendant personal, societal, and economic harm (numerous deaths, ravaged lives, and increased economic harm in the billions of dollars);
- A substantial increase in undetected and unprosecuted public corruption and fraud against the government (in the billions of dollars) and a resulting lost trust in government;
- A substantial increase in undetected and unprosecuted terrorist bombings, murders, and other acts with the attendant loss of numerous lives and billions of dollars in economic harm;
- A substantial increase in unprosecuted criminal cases of all kinds and the potential for a substantial increase in acquittals and hung juries occasioned by the lack of direct and persuasive electronic surveillance evidence.

ELECTRONIC SURVEILLANCE: SURGICAL USE WITHOUT ABUSE

In passing the Title III legislation, codified at 18 U.S.C. 2510–21, Congress enacted a comprehensive electronic surveillance regimen that carefully balanced the communications security needs and privacy rights of individuals with the legitimate needs of law enforcement to protect the public and effectively enforce the law. Above and beyond the traditional requirements of the fourth amendment compliance (such as probable cause, the need for impartial judicial review and a warrant, particularity as to the object of the search, prompt execution of the electronic search, etc.), Congress also specified that electronic surveillance could be used, generally speaking, only as a last resort (when other investigative techniques failed or were too dangerous); only for serious felony offenses; and only for specific criminal communications. The acquisition of noncriminal, nonrelevant communications is forbidden and such communications must be carefully minimized.

Congress has also enacted an electronic surveillance regimen for use in intelligence based investigations, the foreign intelligence surveillance act of 1978 (FISA), codified at 50 U.S.C. 1801–1811. Contrary to the assertions of some, electronic surveillance conducted pursuant to Title III or FISA may *not* be (*and are not*) employed against individuals exercising their first amendment rights, such as by engaging in unpopular, political, or antigovernmental discourse.

An objective review and assessment of the Title III and FISA statutes, and of the conduct of electronic surveillance by law enforcement pursuant to these statutes, indicate that electronic surveillance has been conducted sparingly, judiciously, and in compliance with the letter of the law and the spirit of Congress' intent. As demonstrated by the lives saved and important investigations and prosecutions successfully completed, the Title III statutory regimen has served both society and law enforcement extremely well. Moreover, after 25 years of usage, there is no evidence of significant abuse. Statistics compiled by the FBI, which is charged with investigating violations of the Federal "wiretap" statute based upon acts of illegal electronic surveillance and wiretapping, indicate that instances of illegal wiretapping are very, very rare.

ELECTRONIC SURVEILLANCE TECHNICAL ASSISTANCE

When the Title III legislation was enacted by Congress in 1968, there was no specific provision for technical or other assistance to law enforcement. With regard to wire communications, law enforcement necessarily relies upon the telecommunication service provider's assistance in identifying the target's wire pairs and their line "appearances," and upon the service provider's furnishing of leased lines to enable the intercepted communications to be transmitted to a secure, law enforcement monitoring facility.

Although the service provider assistance requirement was thought to be self-evident and implicit in the Title III legislation, certain service providers initially resisted providing law enforcement with needed assistance, even when directed to do so by court order. *See, e.g., Application of United States,* 427 F.2d 639 (9th cir. 1970). as a result, Congress was compelled to amend the Title III statute in 1970 and expressly fix the assistance responsibility therein. The assistance provision, as amended, and codified at 18 U.S.C. 2518(4), states:

> An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, *direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception* unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefore by the applicant for reasonable expenses incurred in providing such facilities or assistance. (emphasis added)

The FISA statute, enacted in 1978, contains a similar assistance provision, codified at 50 U.S.C. 1805(b)(2). So also do the pen register and trap and trace statutes. *See* 18 U.S.C. 3124(a)(b).

It is very important to understand that telephone companies historically have been extremely conservative, and often have declined to provide law enforcement with necessary technical assistance, even when served with court orders. For example, some telephone companies initially resisted providing law enforcement with even minor "leased line" assistance to allow law enforcement to carry out a pen register investigation, although served with a Federal search warrant. This resistance to pen register assistance was removed by the Supreme Court in *United States* v. *New York Telephone Co.,* 434 U.S. 159 (1977). Some telephone companies also resisted providing relatively minor assistance to effect a trap and trace of dialed number information when served with a Federal court order. Federal court of appeals action was required to obtain such trap and trace assistance to trace dialed number information. *United States* v. *Mountain States Telephone and Telegraph Company,* 616 F.2d 1122 (9th cir. 1980); *In re application of United States,* 610 F.2d 1148 (3rd cir. 1979); *Michigan Bell Telephone Company* v. *United States,* 565 F.2d 385 (6th cir. 1977). The lesson from such incidents is clear: Some telecommunications companies, including common carriers, who are concerned with their legal liabilities will act only when the law is clear as to their responsibilities and when presented with a court order.

In the areas of pen registers and trap and trace devices, courts have required telecommunication service providers to extend technical and physical assistance to law enforcement, in order to effectuate court orders. There are, however, no Federal cases construing the Title III or FISA statutory "assistance" provisions. Attorneys who have analyzed these assistance provisions believe that their current language does not clearly mandate that service providers affirmative must take any steps or develop any technical solutions to accommodate or effectuate a court's electronic surveillance order. Thus, the issue as to the nature and extent of service provider assistance remains an open, and often hotly debated, question.

The question has been raised by some if requesting or requiring greater electronic surveillance technical assistance of service providers to carry out a court order through either hardware- or software-based modifications or developments extends law enforcement's authority. There appears to be general agreement within the government and industry that this would not extend law enforcement's electronic surveillance authority. This agreement extends to law enforcement's legal authority or entitlement to obtain the content of a criminal target's communications or dialed number information transmitted via a telecommunications network.

Some have stated that requiring telecommunication service providers to expend additional technical or monetary resources, even pursuant to court order, to help law enforcement effect electronic surveillance is unwarranted or unprecedented.

However, historically telecommunication service providers have been required to alter their operations and activities to meet law enforcement requirements. For example, service providers have been *required by regulation* to maintain telephone toll records longer than operationally necessary, and generally they dedicate time, human resources, and hence money, to provide law enforcement agencies with such subscriber information. Further, by way of precedent, Congress has enacted public safety/public welfare *legislation* concerning telecommunication service providers in the area of interoperable equipment to assist the hearing-impaired and in the area of telephonically transmitted pornographic communications (so called "dial-a-porn"). Also, many localities *require by law* that the telecommunication local exchange carriers provide "911" emergency service, the cost of which is passed on to all subscribers.

Within the United States, there are numerous other public safety/public welfare laws and regulations which affect a number of industries and businesses and mandate technical efforts and monetary expenses (e.g., required sprinkler systems, smoke detectors, fire alarms, fire escapes, etc., in offices, factories, apartment complexes, etc.; safety belts, "air bags," catalytic converters, and emission control devices in vehicles). On balance, when law enforcement's court-ordered use of electronic surveillance is viewed in terms of its important, and even critical, utility in preventing and solving crimes, and *as a public safety requirement,* there can be no serious doubt that a policy decision requiring such technical assistance *by law* is consistent with past societal and governmental practices.

SUMMARY OF TECHNOLOGICAL IMPEDIMENTS

Prior to 1984, the majority of local and long distance telecommunications were carried by AT&T, which held a virtual monopoly on these services. This resulted in an homogeneous network in which the technologies used to conduct business were the same throughout the network. Additionally, because of an absence of competition, new technologies were introduced slowly and by only a small number of manufacturers.

Since the divestiture of AT&T in 1984, the number of service providers, as well as the diversity of technologies, has grown rapidly and dramatically. For example, the number of carriers providing local telephone service is now over 1,400. A September 1992 decision by the Federal Communications Commission is facilitating even greater competition in this area. As a result, the industry will begin to see new providers of service and already has begun to see new business partnerships among existing service providers. Also, the number of long distance carriers has grown from essentially one in 1984 to over 300 today. With the advent of wireless technologies, such as cellular, the number of service providers grew again. Today, there are over 160 cellular service providers. The introduction of new technologies, as well as actions taken by the Federal courts and the Federal Communications Commission, have resulted in greater numbers and more diversity among service providers. As a result, law enforcement agencies have had to work with many different service providers to obtain the assistance necessary to conduct wiretaps. Numerous situations have arisen where service providers who were inexperienced with court authorized wiretaps have been unable to provide assistance to law enforcement agencies because of a lack of understanding of the legitimate requirements of law enforcement.

Traditionally; common carriers have offered essentially "fixed point" telecommunications: that is to say, communications generated by, or intended for, a customer and transmitted to a fixed location corresponding to a specific telephone number. Historically, these communications have been transmitted over common carrier facilities, such as telephone wires that were dedicated to a customer's specific telephone number (often referred to as a subscriber's "loop"). In the past, when law enforcement agencies conducted court-authorized electronic surveillance or "wiretaps" on a subject's traditional "local loop," they were virtually assured of intercepting the content of all communications (as well as the related dialing information) associated with the subject's telephone number set forth in the court order.

Over recent years, advances in telecommunications technologies, as well as the increasing number of common carriers (approximately 2,000) entering the telecommunications marketplace, have introduced new sophisticated services and features that allow for the efficient transmission of multiple, simultaneous communications of multiple subscribers. Such communications are transmitted over fiber optic lines and wire facilities that previously were dedicated to a single communication and a single subscriber. Other advanced communications services (such as cellular telephones) and features (such as call forwarding which permits customers to redirect calls intended for them) undermine the necessity for communications to be transmitted always to the same specific location or through the same wireline loop. Likewise, "follow-me" features and services expand the notion of call forwarding to national proportions. Further, common carriers' deployment of the Personal Communications Services (PCS) in the near future will enable users to define their own set of subscribed services, use any fixed or mobile terminal or telephone instrument, and initiate and receive calls across multiple networks without regard to their geographic location. All of these "follow-me-type" services, in effect, disassociate a subscriber's number from a fixed local loop. Thus, law enforcement's ability to conduct successfully court-ordered electronic surveillance is greatly hampered.

As a result of these and other new and advanced technologies, common carriers are no longer able to ensure their ability to isolate specific communications (and dialing information) associated with the subjects of court-ordered surveillance, to the exclusion of all other subscribers' communications and dialing information. Industry representatives rave bluntly told law enforcement that the existing telecommunications systems and networks will thwart court authorized intercepts. The above-described services and features and the new telecommunication systems planned for future implementation, both in their current and planned configurations, often prevent, and will continue to prevent common carriers from providing law enforcement with access to all of the communications and dialing information that are the subject of electronic surveillance and pen register court orders.

The attached charts (past operating environment, present operating environment, and future operating environment) depict the increasingly complex telecommunications environment in which law enforcement has operated and will continue to operate when attempting to execute court-authorized electronic surveillances.

Over the last decade, it is conservatively estimated that several hundred electronic surveillance and pen register and trap and trace court orders have been frustrated, in whole or in part, by various technological impediments. During 1993, the FBI, through an informal survey of Federal, State, and local law enforcement, collected information regarding the execution of recent electronic surveillance court orders (including authorizations for call content, pen register, and trap and trace) in order to gauge how many court orders have been frustrated or delayed due to technology-based problems. The survey revealed 91 instances in which law enforcement agencies participating in the survey were precluded from implementing or fully implementing court orders for electronic surveillance due to various technological impediments. The majority of the problems were encountered during attempts to execute orders regarding electronic surveillance activities relating to cellular telephone systems (33 percent) and "fixed" or wireline communications that employed custom calling features (32 percent). With respect to cellular systems, problems have ranged from a technical inability on the part of the cellular common carrier to assist law enforcement, to cellular systems that were not capable of isolating and collecting communications and/or pen register information (dialed numbers) associated with subject's telephone communications. A separate category of technical problems associated with cellular systems relates to the inability of some cellular carriers to comply with court orders due to a limited capacity associated with the carrier's particular system (11 percent). The following are examples to illustrate some of the impediments encountered:

1) A federal investigation of a major narcotics organization operating in the northeastern United States was hampered when the cellular telephone service provider was unable to fulfill requests for court-ordered wiretaps due to the provider's technical limitations.
2) An organized crime and drug trafficking task force investigation in the southeastern U.S. was unable to conduct a court-ordered wiretap as the cellular telephone service provider was unable to provide law enforcement with access to the subject's long distance communications made through the providers cellular service.
3) Two different cellular service providers in the mid-western U.S. were unable to comply with separate federal court-orders requesting pen register or dialed number information from a suspected drug trafficker's cellular telephone.
4) A regional telephone company in the mid-western U.S. was unable to provide a federal law enforcement agency with the content and dialed number information from a suspected drug traffickers telephone as a result of the subjects use of custom calling features.
5) A cellular service provider in the south was unable to comply with a Federal court-order for dialed number information concerning a Federal public corruption investigation due to technical limitations.

It is important to note that there have been many instances where court orders have not been sought or served on carriers due to law enforcement's awareness of these preexisting impediments, and therefore they were not tabulated in connection with this survey. Included in a recent letter from the director of a high intensity drug trafficking area (HIDTA) it was noted that a Federal law enforcement agency did not pursue twenty-five court orders because of the known inabilities of the cellular service provider to effectuate such orders.

However, it would be a mistake to analyze and respond to this problem simply by attempting to count the specific number of court orders frustrated or delayed in the past. Although they convey a sense of the problem, and identify some of the technical problems that are being encountered as a result of recent telecommunications technology advances, focusing on these numbers and technologies alone is terribly misleading. Fortunately, the number of court-ordered interceptions that have been impeded by technology is still somewhat limited. However, the telecommunications technologies that are emerging will likely have a much greater and more devastating impact on law enforcement's ability to conduct court-ordered electronic surveillance in the future.

FBI/GOVERNMENT EFFORTS TO OBTAIN TELECOMMUNICATIONS INDUSTRY'S COOPERATION/SOLUTIONS

For almost four years, the government has attempted to resolve the technical issues associated with court-ordered electronic surveillance by meeting with various representatives of the telecommunications industry at virtually all corporate levels. Historically, law enforcement's interface with this industry has been through the security organization of the common carrier. It is this interface that previously has been most knowledgeable of law enforcement's electronic surveillance requirements, as they receive court orders requiring them to assist law enforcement with their electronic surveillance responsibilities. However, it was learned in 1990, during discussions with the industry, that the security entities within the common carrier companies were not routinely involved in the industry's technology planning, design, and development processes. As a result, law enforcement's needs were not being incorporated into the carriers' system requirements.

In an attempt to have law enforcement's requirements considered during the industry's planning processes, the government systematically met with the most senior levels of the traditional common carriers and briefed them about the difficulties being encountered by law enforcement and about our concerns that future technologies would severely diminish, if not preclude, this critical investigative technique. Although these executives appeared supportive of law enforcement's goals, several of them indicated that without some sort of mandate, such as legislation, their companies could not unilaterally invest time, money, and technical resources in developing and implementing solutions, especially if there were no assurance that their competitors would do so.

On January 15, 1992, then President Bush authorized the Justice Department to proceed with a legislative initiative. On March 6, 1992, the digital telephony legislation was announced, and the industry response was generally negative, a position that was at variance with that expressed previously by a number of the representatives of the telecommunications companies. On March 18, 1992, then Attorney General William Barr and then FBI Director William S. Sessions sponsored and chaired a meeting for all major industry executives. It was attended by four telecommunications executives, representing the industry. During this meeting, telecommunications executives asserted that the FBI had been talking to the wrong people in industry (the security officers, senior executives, etc.) and that the solution to these problems rested with those upper/mid-level managers and engineers who oversaw development/implementation of the technologies in question. The Attorney General agreed to an industry request that a telecommunications technical committee consisting of the "right industry people" (picked by the CEOS) be created to identify technical solutions and to get the job done. It was also clearly understood that the administration and law enforcement would continue to pursue legislation.

As a result of the March 18, 1992, meeting, industry representatives met with the government on March 26, 1992, to begin a process of establishing a technical working committee to address technical impediments to electronic surveillance. In May of 1992, an ad hoc technical working group began. This group was later organized as the electronic communication service providers committee under an industry association now known as the Alliance for Telecommunications Industry Solutions (ATIS). This committee consists of representatives of electronic communication service providers (e.g. common carriers), telecommunications equipment manufacturers, and law enforcement officials, who attend voluntarily and with varying degrees of regularity and interest. As a result of this process, over the past two years there has been a better understanding by both law enforcement and industry representatives of the issues that each face with respect to electronic surveillance. However, contrary to assertions, new telecommunications technologies will jeopardize law enforcement's surveillance abilities. The ATIS chairman has stated in a recent letter that the entire committee, not just one participant or one group of participants, now recognizes the problems and impediments that these telecommunications technologies are creating for law enforcement. A copy of our correspondence with the ATIS chairman is attacked as an exhibit.

I support continued dialog between industry and law enforcement. However, it must be recognized that this committee process is *voluntary* and, as such, only those companies who are committed to assisting law enforcement participate and support this effort. Second, only a handful of the over 2,000 companies attend. Third, no implementable solutions have been developed since discussions began almost two years ago. Fourth, committee resolutions are nonbinding and it is not possible to secure a commitment from participants to *implement* any solutions that may be developed in this voluntary forum. Finally, as in any business decision, it is recognized that there will be costs incurred by industry to accommodate law enforcement's requirements. The ATIS chairman has also indicated that antitrust and other legal considerations preclude discussions and resolutions to these cost issues. In light of these limitations, the administration and all of law enforcement have concluded that the committee process is not, and cannot be, a substitute for a legislative mandate to ensure law enforcement's continued ability to conduct court-authorized electronic surveillance.

PRESIDENTIAL REVIEW DIRECTIVE (PRD)

In April 1993, President Clinton directed that an interagency working group be established under the auspices of the National Security Council (NSC) to examine advanced telephony and to consider its effect and impact on the conduct of electronic surveillance by our nation's law enforcement and intelligence agencies. After an in-depth eight month study, the NSC provided a number of policy options for the Vice President and appropriate cabinet officials. As a result of their review of the options, it was unanimously decided that comprehensive legislation was the only effective way to deal with the "digital telephony" problem. Fundamental to this decision was the belief that it would be unacceptable for the safety of the American public to be imperiled, the national security endangered, and effective law enforcement eroded through the loss or diminishment of this critical and essential tool of our nation's law enforcement and intelligence agencies.

PROPOSED LEGISLATION

The proposed legislation represents, in our estimation, the only rational and viable approach to solving the digital telephony problem in a comprehensive fashion. Only through legislation can the government be assured that within a reasonable period of time the impediments to electronic surveillance will be removed and our society's window of vulnerability closed. Without enactment of the administration's proposal, one of our most effective weapons against national and international drug trafficking, terrorism, espionage, organized crime, and serious violent crimes will be severely and adversely impacted. Without its enactment, the public safety, the national security, and effective law enforcement will be imperiled.

The purpose of this legislation is to maintain technological capabilities commensurate with existing statutory authority—that is, to prevent advanced telecommunications technology from repealing *de facto* the statutory authority already conferred by the Congress. The proposed legislation explicitly states that the legislation does not enlarge or reduce the government's authority to lawfully intercept the content of communications or install or use pen register or trap and trace devices pursuant to court authorization. Neither does it alter the current duty of the service provider to assist law enforcement and receive payment for such assistance. Nor does it alter existing causes of action, civil liability, or good faith defenses.

The "purpose" section of the act indicates that the act is designed to clarify and define the responsibilities of common carriers, providers of common carrier support services, and telecommunications equipment manufacturers. They would be requested to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information (e.g., dialed number information), pursuant to the Federal and State electronic surveillance and pen register and trap and trace statutes. The "assistance" requirement that is clarified and more fully defined is not a new one, but rather a long-standing one, dating-back to 1970. In the original assistance provision, Congress evidenced a clear intent that lawful court orders should not be frustrated due to a service provider's failure to provide needed technological assistance and facilities. The proposed legislation clarifies and defines the *nature* and *extent* of the responsibility which arises from the unequivocal mandate of the 1970 law.

An additional purpose of the act is to improve communications privacy protection for users of cordless telephones, certain radio-based data communications and networks, communications transmitted using certain privacy-enhancing modulation techniques, and to clarify the lawfulness of quality control and service provision monitoring of electronic communications on a par with wire communications.

The legislation sets forth law enforcement's electronic surveillance requirements. The requirements are, by design, generic in nature and are intended to put common carriers on notice as to needs of law enforcement. The government purposely eschewed setting any technical standards because it does not desire to "dictate" particular technological solutions. It is the government's position that each common carrier is best positioned and qualified to determine how it will meet the requirements in the most cost-effective way.

The articulation of these requirements constitutes the first legislative listing of law enforcement's electronic surveillance requirements. However, most of these requirements have been known to the major local exchange carriers, interexchange carriers, and cellular carriers for quite some time.

In brief, the requirements specify that common carriers must be able to provide forthwith, pursuant to court order or lawful authorization, the capability and capacity to permit the government to conduct electronic surveillance, pen register, and trap and trace investigations effectively. Common carriers are required to ensure that there is an ability to execute expeditiously and simultaneously all court orders and lawful authorizations directed to them. Second, they are required to ensure that the content of communications and call setup information (dialing information) can be intercepted, acquired, and provided to the law enforcement agency. It must be provided concurrent with the transmission of the subject's communication, to the exclusion of anyone else's communications or dialing information, and without regard to the mobile nature of the facility or service that is the subject of the court order or lawful authorization, regardless of any features offered by the common carrier used by the subscriber who is the subject of the court ordered intercept. Third, they are required to sure that communications can be intercepted and dialing information acquired unobtrusively and with a minimum of interference with any subscriber's telecommunications service. Finally, they are required to ensure that the content of communications and the dialing information can be transmitted to a location identified by the government distant from the facility that is the subject of the interception, from the interception access point, and from the premises of the common carrier.

The basis for these requirements is easy to understand. Inasmuch as communication interceptions and dialed number acquisitions increasingly will be activated from within common carrier premises, including switching offices, it is critical that there be sufficient capacity to accommodate completely the concomitant needs of all law enforcement and government agencies.

It is critical for law enforcement agencies to be able to intercept communications and acquire dialing information concurrently, so they can respond immediately to life-threatening circumstances and react promptly and effectively to criminal activity in terms of making needed arrests, seizing evidence, and interdicting contraband, such as drugs, illegal weapons, and bombs. This requirement also is important and critical in helping law enforcement agencies "minimize" the monitoring and recording of noncriminal communications.

The requirement that common carriers have the ability to isolate for law enforcement the communications and dialing information of the subjects of electronic surveillance to the exclusion of the communications and dialing information of other subscribers is a basic and a long-standing one. Law enforcement agencies do not want to be faced with the prospect of having to "sort through" a tangle of communications which include the communications of innocent individuals who have the misfortune of having their communications "bundled" or otherwise commingled with those criminal conversations of the subject of court-ordered interception in the telecommunications transmission process. (However, if the "bundling" of communications is being done by the subscriber law enforcement does not expect the common carrier to "unbundle" these communications. This ability is being challenged by the increased use of digital transport, multiplexing, and fiber optics closer to the premises of the interception subject.

The requirement pertaining to the mobile nature of services and features directly addresses the significant impediments to electronic surveillance brought about by cellular, Personal Communications Services (PCS), and other emerging mobile services, as well as features and services which permit subscribers to program or otherwise direct communications to any facility they choose (e.g., "call forwarding" and "follow me service").

The basis for the requirement that communications and dialing information be acquired unobtrusively and with a minimum of interference with any subscriber's service is self evident. Without it, electronic surveillance would be detected by the subject of the intercept and compromised.

The requirement that intercepted communications or acquired dialing information be received at a location identified by law enforcement agencies distant from the subject's facility, from the interception point, and from the premises of the common carrier is likewise not new and maintains current operating procedures. This requirement is fundamentally important, since without it the safety of law enforcement officers and government employees would be put at risk, the interception easily could be compromised through detection, and the effective execution of the surveillance would be significantly disrupted.

The legislation contains a provision entitled "systems security" which is intended to maintain the highest levels of telecommunications privacy and systems security. Since communication interceptions and dialing information acquisitions increasingly will be facilitated from within common carrier premises, including switching facilities and network elements, it is critical that these facilities remain highly secure. Consequently, law enforcement will be required to notify common carriers of any interceptions that are to be effected within such facilities. Further, common carriers will designate individuals who exclusively will have the ability to activate all such interceptions for law enforcement. Law enforcement and other government agencies are not seeking the authority or ability to remotely activate interceptions within the premises of a common carrier in a fashion that bypasses personnel designated by common carrier. All executions of court orders or authorizations which require access to the switching facilities or other carrier premises will be made *through* the individuals authorized and designated by the common carrier.

The focus of compliance is upon common carriers within whose networks most of the electronic surveillance occurs and where most of the impediments are encountered. Compliance is set for within three years, a period of time considered to be reasonable for removing the impediments. The coverage of compliance includes only needed modifications to existing systems and networks, as well as to future systems and networks (those fielded after the three-year compliance period).

Because common carriers must rely on equipment manufacturers and support service providers, the legislation provides that common carriers are to consult with these entities in a timely fashion and that these entities, in turn, shall make available needed equipment and services on a timely and priority basis, and at a reasonable and cost-effective charge.

Enforcement of the legislation is vested in the Attorney General. This is to avoid disparate enforcement actions throughout the country in ways that could be burdensome for common carriers. The Attorney General is authorized to seek injunctive relief against common carriers, equipment manufacturers, and support service providers, as well as to file civil actions for fines against common carriers. The Attorney General is also authorized to request enforcement assistance from the Federal Communications Commission. Violators are subject to a civil penalty of $10,000 per day for each day in violation. As a practical matter, it is not expected that these enforcement remedies and actions will be required, particularly with. Regard to responsible common carriers. However, with approximately 2,000 common carriers now in the telecommunications marketplace, the prospect that some will disregard these requirements or respond to them in a dilatory fashion cannot be disregarded.

In order to facilitate compliance with the provisions of this legislation, the Attorney General is encouraged to consult with the Federal Communications Commission and common carrier representatives and to utilize common carrier standards bodies, associations, or other such organizations to discuss details of the requirements and cost-effective approaches.

In the definition of the term "intercept," it is made clear that the legislation, as a general rule, does not make common carriers responsible for deciphering or decrypting encrypted communications. As a general rule, law enforcement agencies assume this responsibility. Common carriers are required to provide only the plaintext of encrypted communications when the encryption was provided by the common carrier the common carrier possesses the information necessary to decrypt the communication.

The term "call setup information" is essentially the dialing information associated with any communication which identifies the origin and destination of a wire or electronic communication obtained through the use of a pen register or trap and trace device pursuant to court order. It does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent whatsoever, with reference to this term, to acquire anything that could properly be called "tracking" information.

The legislation includes several provisions that are intended to improve communications privacy. These include the conferral of full privacy protection for cordless telephones, including those transmissions occurring in the radio link between the telephone handset and base station. This provision recognizes that newer generations of cordless telephones tend to afford greater privacy protection to users than those previously marketed, because lawful network monitoring is allowed for electronic as well as wire communications.

It is important to understand that this legislation is intended to stand the test of time and overcome the shortcomings of the 1970 amendment. It is specifically designed to deal intelligently and comprehensively with current and emerging future telecommunications technologies and to preclude the need for much more restrictive and more costly legislation in five or ten years when court-authorized interceptions would no longer be possible due to further technology advances. Any legislation that would limit its application to technological impediments on a "piecemeal" basis would be disastrous. Piecemeal legislation which deals only with current problems or some of the problems would result in common carriers fully deploying new technologies which would impede electronic surveillance and which would cause the government to return to the Congress repeatedly. In the meantime, the public safety, the national security, and effective law enforcement would be harmed and the cost of removing those future impediments would be prohibitive. Indeed, in this regard, bad legislation would be worse than no legislation at all.

WHAT THE LEGISLATION DOES NOT PROPOSE

Much of the criticism directed toward the administration's proposal has been misleading or incorrect. I would like to clarify for the record what the legislation does *not* propose.

NO CHANGE IN LEGAL AUTHORITY

First, as I previously stated, the proposed legislation does not seek to expand the current laws authorizing the interception of wire or electronic communications. To the contrary, this proposal simply seeks to maintain law enforcement's ability to conduct the types of surveillances currently authorized in Chapters 119 and 206, Title 18, U.S.C.; the foreign intelligence surveillance act; and the laws in 37 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. In 1968, Congress carefully considered and passed legislation setting forth the exact procedure by which law enforcement can obtain court authorization to conduct electronic surveillance. The statute demands that law enforcement use electronic surveillance only as a technique of last resort. Requests for electronic surveillance receive rigorous administrative and judicial scrutiny and are granted only after a Federal District Court judge, or his/her state/local counterpart, is satisfied that all the statutory safeguards have been met and all other reasonable investigative steps have failed, or are likely to fail. The proposed legislation will not change this.

Furthermore, service providers will not execute an intercept without the required court order or statutory authorization. Any attempt to do so by anyone, either inside the government or the private sector, will continue to be a violation of Federal law and those individuals will be prosecuted to the fullest extent of the law.

In addition, the proposal will not change who controls access to the communications to be intercepted. In fact, interception access points increasingly are likely to be activated within the common carrier's premises, thereby severely limiting the potential for illegal wiretapping. The proposal will *not* open the door to easy or wholesale wiretapping, nor does law enforcement envision a marked increase in the number of electronic surveillance court orders that will be sought or an increase in the types of investigations in which a court-authorized interception can be granted. The legislation does not, in any way, relax the established statutory and court-imposed requirement for obtaining a court order.

This proposal does not restrict technology. It deals solely with *preserving* technical capabilities. The proposed legislation seeks only to clarify and more clearly define existing law regarding the "technical assistance" provision by making it applicable and meaningful, regardless of the technology employed.

ENCRYPTION

The proposal, in essence, only addresses the technological issue concerning *access* to communications and does not alter the legal requirements currently associated with court-ordered intercepts. With minor exception where encryption was provided by the common carrier and the common carrier possess in the information necessary to decrypt the information, the legislation does *not* address the issue of encryption. While encryption certainly poses a problem for law enforcement, this legislative proposal focuses only on the issue of interception access within advanced communications networks. The topic of access within advanced telecommunications networks is distinct from encryption and poses an immediate and critical problem for law enforcement for which we are now seeking a legislative solution.

NETWORK SECURITY AND RELIABILITY

Some have raised concerns regarding the impact this legislation might have on network security and reliability. Certain special interest spokespersons have asserted that the legislation will make it easier for anyone, from computer hackers to foreign spies, to access an individual's communications. These fears are unfounded and misplaced. First of all, just as network maintenance and audit access can be accomplished with full regard for network and system security, so also can law enforcement's electronic surveillance access be accomplished with the same high regard for security and privacy. Second, the proposed legislation includes a "systems security" provision which means that only designated telephone company employees will activate interceptions which originate within telephone company premises. Third, unauthorized access to communications remains a serious crime which is addressed in the current electronic surveillance statutes. Any unauthorized individual or group breaching communications security and privacy is subject to prosecution to the fullest extent of the law. Fourth, this proposal will not introduce any vulnerabilities into systems that are not already present. As technology evolves and as any new features and services are introduced, industry will necessarily plan network security measures and countermeasures early in the design phase and address intensively the architectural design for network security.

The proposed legislation fits well within the context of these activities. By requiring common carriers to develop law enforcement access solutions within their own networks, we are best assuring appropriate security. Therefore, contrary to many public statements made on the subject, law enforcement is not seeking to build "back doors" to sneak into common carriers' systems. The proposed legislation is not some dreaded Orwellian prophecy come true. Rather, this legislative proposal represents a recognition of legitimate law enforcement needs and a desire to protect the American people.

To support normal operations, service providers must manage and maintain their networks. This is terribly important to the FBI just as it is for everyone. Law enforcement electronic surveillance interception access to communications will be a stringently controlled extension of the system's features. With adequate planning, the integration of law enforcement's needs should be easily accommodated within the requirements for network security. *To further enhance the public's confidence in the security of our communications networks, subcommittee staff have raised with us the issue of imposing reporting and auditing requirements on common carries concerning their implementation of authorized intercepts. We are supportive of such requirements.*

EFFECTS ON NETWORK DESIGN AND TECHNOLOGY

Another concern that has been raised is the possible negative impact this legislation might have on network design and technology, requiring a broad re-engineering of the network components. The proposed legislation does not require common carriers to design their systems in any one, particular way. The proposal simply requires that common carriers respond to the generic requirements of law enforcement and provide law enforcement with interception access and the capability and capacity to intercept wire and electronic communications, in real time, when authorized by law.

This legislation also does not propose that industry design systems with the ability to wiretap as the "design goal." Law enforcement is simply requiring common carriers to craft appropriate solutions that interface with their networks' designs. Industry is in the best position to develop reasonable and cost-effective solutions and, at the same time, maintain the security and reliability of the networks.

Furthermore, we are unaware of any authoritative industry statement that these requirements would significantly delay development of new technologies.

Additionally, this legislation does not prohibit or impede the deployment of new telecommunications technologies. Advanced technologies support a number of features that make systems more intelligent. The basic technology underpinning the introduction of advanced features and services, which often impede electronic surveillance, likely will offer solutions to these very problems.

Law enforcement's requirements will not dictate the course or pace of technology. However, with this legislation, our requirements intentionally will be included, rather than excluded, in the development of new technology in much the same fashion that other legislation requires new technologies and products to take public safety into account.

COMPETITIVENESS

Another issue raised pertains to the effect of the legislation on American competitiveness. The proposed legislation will not in any fashion adversely affect competitiveness. Domestically, the proposed legislation would mean that all 2,000 common carriers would compete on a "level playing field" because all providers would be required to meet the sane electronic surveillance specifications. The proposed legislation does not prohibit U.S. manufacturers or international service providers from developing or deploying equipment or service features for sale outside the United States that are different from that required pursuant to the proposed legislation. This proposal only applies to common carrier communications services *deployed* within the United States. If anything, this legislation could provide U.S. industry with a competitive edge. Other democratic nations will very likely want telecommunications systems and equipment that preclude service providers from developing or deploying equipment or service features not capable of intercept.

PRIVACY-BASED OBJECTIONS

A spokesperson for the American Civil Liberties Union (ACLU) has stated on numerous occasions that the ACLU opposes the proposed legislation because it would allow law enforcement to maintain technical capabilities commensurate with existing federal and state legal authorities. This is because the ACLU opposes the existing legal authorities—those found in the Title III and FISA statutes, as it persists in the erroneous position that wiretapping is unconstitutional per se. This radical position is in flat opposition to the policy positions and the constitutional analyses of the executive, legislative, and judicial branches of both the Federal and State Governments. The United States Supreme Court held long ago that the Title III wiretap statute *is* constitutional. See *United States* v. *Donovan,* 429 U.S. 413 (1977).

Privacy is protected in the federal and state electronic surveillance statutes by requiring law enforcement agencies' adherence to a number of legislatively-created protections that far exceed the fourth amendment requirements relating to court orders based upon probable cause.

In fact, the proposed legislation contains a number of privacy-enhancing provisions, such as extending full privacy protection to cordless telephones, radio-based electronic communications, and communications transmitted using privacy-enhancing modulation techniques.

THE FALSE "TRANSACTIONAL DATA SCARE"

The Digital Privacy and Security Working Group (DPSWG) has attempted to interject a false "transactional data scare" into the current discussion of the need for legislation that will allow law enforcement to maintain its electronic surveillance and pen register/trap and trace technical capabilities commensurate with existing law.

In a letter to me, dated March 11, 1994, a copy of which was sent directly to the chairmen, the DPSWG falsely alleges that we are seeking to "dictate to industry" a *new* capability to acquire "minute-by-minute surveillance of individuals" through transactional data. This is a false issue for a number of reasons.

First, as is clearly set forth in the "purpose" section of the proposed legislation, the intent of the legislation is to maintain existing technical capabilities and to "clarify and define the responsibilities of common carriers * * * to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information *under Chapters 119 and 206 of Title 18 and Chapter 36 of Title 50.*" (emphasis added.) These chapters have nothing to do with "transactional information" under our federal electronic surveillance and privacy laws. All telecommunications "transactional" information is already protected by Federal law and is exclusively dealt with in Chapter 121 of Title 18 of the United States Code ("stored wire and electronic communications and transactional records access"). The proposed legislation does not relate to Chapter 121 of Title 18.

Second, under federal law, Congress treats law enforcement's use of pen registers and dialing information differently than "transactional information"—such as detailed telephone *billing* information. The dialing information derived from a pen register is obtained by law enforcement and is limited to a *specific telephone line and number.* On the other hand, transactional billing information is compiled by telephone companies and captures billing information from *every telephone a subscriber may use* during the billing period, such as credit card calls, collect calls, operator assisted calls, and third number billing information which are associated with all the different telephones a subscriber may use.

Third, Congress has enacted legislation that requires law enforcement to obtain a court order in order to obtain "call setup information" through the use of a pen register or trap and trace device, based upon a certification of an attorney for the government that the information likely to be obtained is relevant to an ongoing criminal investigation. Such court orders last for up to sixty days. Any renewal requires the approval of an appropriate judge. On the other hand, Congress has legislated that "transactional information" can be obtained through a number of legal processes, including subpoenas, without resort to court orders. Subpoenas for transactional information typically cover periods of six months or longer. In any event, law enforcement is not authorized to obtain noncriminal, irrelevant information about any individual, and any acquisition of transactional information or dialing-type information must be grounded in relevancy to a criminal investigation or inquiry.

Fourth, the letter indicates that enactment of this legislation, with regard to maintaining our ability to lawfully acquire call setup (dialing) information pursuant to court order, will somehow permit law enforcement to acquire some new information that is not now available. That is simply untrue. This legislation ensures a maintenance of the status quo as it relates to legal authorities under Chapters 119 and 206 of Title 18 and Chapter 36 of title so, and as it relates to the types of information obtainable through pen register and trap and trace devices used pursuant to the court order.

Fifth, unlike the government's proposed legislation, which specifically asserts no intention to alter the existing laws regarding the conduct of electronic surveillance and the installation and use of pen register and trap and trace devices, the DPSWG, by interjecting a false transactional data scare, is apparently seeking to repeal Chapter 206 of Title 18 and the pen register and trap and trace authorizations found in Chapter 36 of Title 50. As explained above, call setup information (that is dialing information) is obtained through the use of pen register and trap and trace devices. In the DPSWG letter referred to above, it states: "legislation should apply to 'call setup information' only when that information is incident to a warrant issued for wire, oral, or electronic communications as set forth in 18 U.S.C. 2518 (Title III)." To accept this radical position on privacy would mean, for example, that anytime an FBI agent simply sought to acquire a telephone number dialed by a criminal subject through the use of a pen register, he/she should be required by law to draft a 30–40 page title iii affidavit, and send it to Washington, DC, for the Deputy Assistant Attorney General of the criminal division to review and authorize, before taking it to a Federal District Court Judge for review and approval. Frankly, such a notion is absurd and is wildly inconsistent with current law.

ALLEGATIONS OF "TRACKING" PERSONS

Law enforcement's requirements set forth in the proposed legislation include an ability to acquire "call setup information." This information relates to dialing type information—information generated by a caller which identifies the origin, duration, and destination of a wire or electronic communication, the telephone number or similar communication address. Such information is critical to law enforcement and, historically, has been acquired through use of pen register or trap and trace devices pursuant to court order.

Several privacy-based spokespersons have criticized the wording of the definition regarding this long-standing requirement, alleging that the government is seeking a new, pervasive, automated "tracking" capability. Such allegations are completely wrong.

Some cellular carriers do acquire information relating to the general location of a cellular telephone for call distribution analysis purposes. However, this information is not the specific type of information obtained from "true" tracking devices, which can require a warrant or court order when used to track within a private location not open to public view. *See United States* v. *Karo,* 468 U.S. 705, 714 (1984). Even when such generalized location information, or any other type of "transactional" information, is obtained from communications service providers, court orders or subpoenas are required and are obtained.

In order to make clear that the acquisition of such information is not being sought through the use of a pen register or trap and trace device, and is not included within the term "call setup information," we are prepared to add a concluding phrase to this definition to explicitly clarify the point: "* * *, except that such information [call setup information] shall not include any information that may disclose the physical location of a mobile facility or service beyond that associated with the number's area code or exchange."

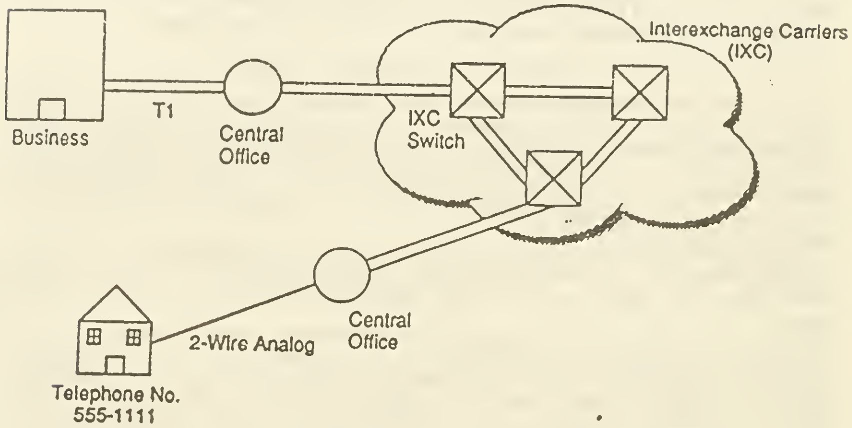
TITLE III INTERCEPTIONS[1]

Year	Original interception applications authorized			Reported results	
	State	Federal	Total	Arrests	Convictions[2]
1982	448	130	578	2,870	1,886
1983	440	208	648	2,890	2,007
1984	512	289	801	3,719	2,429
1985	541	243	784	4,178	2,616
1986	504	250	754	3,830	2,447
1987	437	236	673	3,225	1,956
1988	445	293	738	3,830	2,404
1989	453	310	763	4,199	2,205
1990	548	324	872	3,167	1,327
1991	500	356	856	2,189	2,185
1992	579	340	919	2,685	607
Total	5,407	2,979	8,386	36,782	22,069

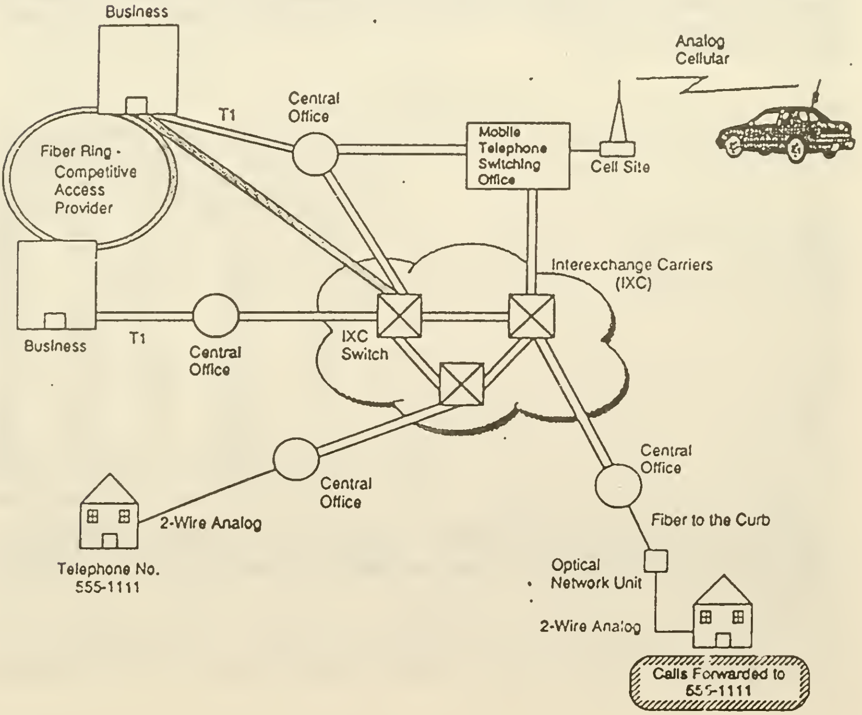
[1] Administrative Office of the United States Courts, Report on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications (Wiretap Report) (1983–1992).

[2] A substantial number of prosecutions are ongoing and total convictions will not be reported for several years. Convictions continue to be reported as a result of interceptions going as far back as 1982. Unfortunately, the reporting of convictions appears to lag substantially behind the actual convictions and there are indications that convictions that should be reported by State prosecutors and judges are not actually reported.

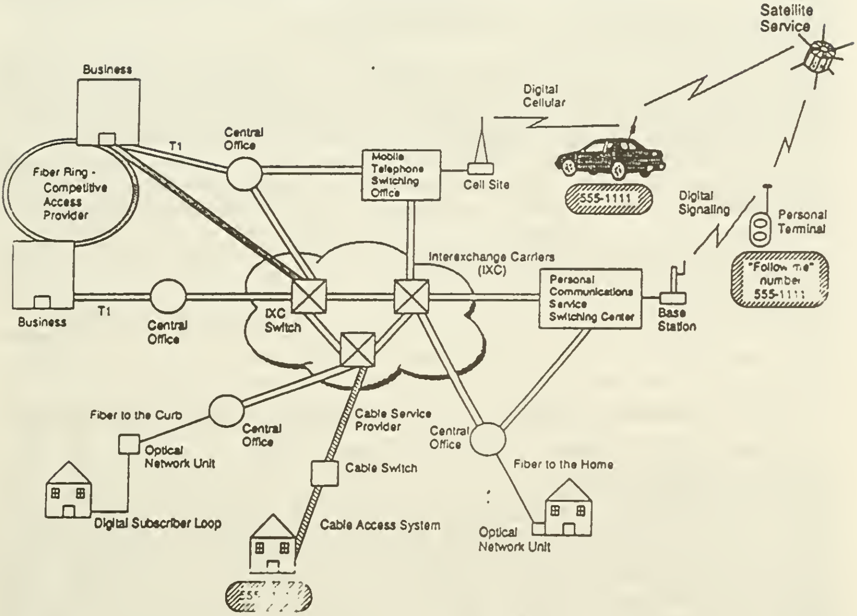
PAST OPERATING ENVIRONMENT



PRESENT OPERATING ENVIRONMENT



FUTURE OPERATING ENVIRONMENT



U.S. DEPARTMENT OF JUSTICE,
FEDERAL BUREAU OF INVESTIGATION,
Washington, DC, May 10, 1994.

Hon. PATRICK J. LEAHY,
Chairman, Subcommittee on Technology and the Law,
U.S. Senate, Washington, DC.

DEAR PAT: Enclosed please find our responses to the questions both you and Senator Pressler had regarding the Administration's proposed "Digital Telephony and Communications Privacy Act of 1994" which were forwarded to me in your two letters dated March 24, 1994. Pursuant to discussions with Subcommittee staff, specific information concerning the Bureau's informal survey which identified ninety-one instances where law enforcement's electronic surveillance were frustrated due to advanced telecommunications technologies will be forthcoming under separate cover.

Should you have any questions concerning this or any other issue of mutual concern, please do not hesitate to contact me.

Sincerely yours,

LOUIS J. FREEH,
Director.

LOUIS J. FREEH'S RESPONSES TO QUESTIONS SUBMITTED BY SENATOR PRESSLER

Question. Why is further legislation necessary? What is lost now that will be gained by this legislation?

Answer. There is no disagreement that under current law telecommunications companies and others are mandated to assist law enforcement agencies execute court orders for electronic surveillance and pen registers/trap and traces, pursuant to court orders directing them to do so. The issue is the nature and extent of that mandate. The current language of the "assistance provision" in the various federal electronic surveillance and pen register/trap and trace statutes, though unambiguous in its mandate, is silent on (and therefore gives no guidance concerning) *what level of effort or level of cost,* if any, must be expended by a provider when its system, as deployed or planned, does not readily accommodate execution of electronic surveillance or pen register/trap and trace court orders, or, when impediments are encountered, how quickly an effort must be undertaken and completed.

Attorneys for the FBI, Bellcore, and the telecommunications industry believe the current language does *not* clearly define the responsibilities of service providers, particularly when some level of effort is required beyond the rudimentary furnishing of line information and leased line facilities. The current language was adequate when enacted in 1970, since telephony technology then was relatively simple and there were relatively few service providers. Today's telecommunications marketplace is vastly different, more complex, and abounding with service providers (e.g., over 2,000 common carriers alone).

Hence, it is imperative that the generic electronic surveillance requirements of law enforcement be articulated formally, that common carrier responsibilities be spelled out, and that a reasonable compliance period be set. Legislation is the only way to put *all* common carriers on notice regarding these requirements and to legally obligate the over 2,000 carriers to act in a timely and comprehensive fashion. Further, legislation is needed in order to formally enlist the cooperation of support service providers and equipment manufacturers upon whom common carriers rely for provisioning service. So also it is necessary to define the government's legal and equitable remedies regarding common carriers who fail or refuse to comply or who are dilatory, and to provide a mechanism for reimbursement to common carriers for costs expended in making the modifications associated with achieving compliance.

If there were any doubt about whether new legislative language is needed to clarify and memorialize the above-mentioned requirements and responsibilities, one need only consider the complaints and false accusations made by some opposition spokespersons concerning the *proposed legislation's memorialization of law enforcement's long-standing requirements.*

A detailed statement of the inadequacy of the current "assistance provision" language is set forth at pages 24–27 of Director Freeh's statement submitted for the record.

Question. How much of a problem is this today? In how many actual cases, roughly, has the FBI been unable to accomplish a court-approved wiretap due to a telecommunications company's inability to make the tap?

Answer. The problem, though hard to quantify, is significant and is clearly growing. The informal FBI survey documented 91 such problems, but there have been many more. Over the last decade, we estimate that several hundred court orders have been frustrated or were not sought because of these problems.

With the introduction and growth of cellular telephone systems, and the introduction and use of sophisticated features and services, the number of court orders for electronic surveillance and/or pen register/trap and traces that were frustrated, in whole or in part, or delayed, or were not sought, grew. With the on-going introduction of even newer, more sophisticated features and services, wireless systems, etc., the number of technological problems will grow at an accelerated rate and the ability of law enforcement agencies to fully and properly execute these court orders will continue to erode.

There is no single repository for information regarding the number of court orders that could not be properly executed with regard to the hundreds of criminal Title III wiretap and thousands of pen register court orders executed each year by hundreds of law enforcement agencies throughout the U.S. it was precisely this circumstance that led the FBI to conduct an informal survey in 1992 to attempt to gather some data, however imprecise, regarding this serious problem. This informal survey disclosed 91 "recent" problems. Information regarding these problems was retrieved by FBI field office Technically Trained Agents (TTAs), and most of the information reported on pertained to FBI cases. It is unclear how effective these TTAs were in obtaining sensitive information from state and local law enforcement authorities about problems they were encountering in executing court orders, particularly regarding then pending electronic surveillance efforts.

The FBI relies upon Technically Trained Special Agents (TTA) throughout the United States to technically implement the execution of the court orders. This duty also involves technical liaison with the telecommunication companies. Problems encountered by these TTAs are sometimes brought to the attention of FBIHQ through requests from the field TTAs for assistance from the FBIHQ's Engineering Section. It is usually through these requests that such problems become known, though they are not tabulated. In addition to the court orders that cannot be executed (fully executed), many requests for electronic surveillance or pen registers/trap and traces by field office Special Agents have been discouraged by the TTAs in a number of field offices due to known on-going impediments in a particular area that have frustrated court orders in the recent past. Thus, a significant number of requests were never pursued and never reached the stage of being submitted for court approval. Such "discouraged" requests are not reported formally to FBIHQ and they were not counted in the survey. A third category of problems are those where court orders have been delayed due to capacity limitations within the telecommunications companies' switches. Although such court orders may ultimately be executed, they may be delayed to the point where critical and valuable information is lost or not collected. Finally, there have been a great number of court orders that are not successfully executed because of problems that do not permit the *comprehensive* interception and acquisition of the subject's communications and/or "call setup information" (dialing information), and therefore have been of limited investigative value. See pages 29–35 of Director Freeh's statement for the record regarding this issue.

Question. Is the problem that the technology is too sophisticated or is it that the companies do not provide adequate access points?

Answer. Generally, the latter. The level of sophistication of the new technology is not viewed as a problem. To the contrary, the sophisticated switches and equipment being developed and deployed today are more capable than the less sophisticated switches that have been in use for many years. As service providers deploy more sophisticated switches, they develop more sophisticated features and services in response to or in anticipation of the commercial demands of their customers. If service providers view the electronic surveillance requirements of law enforcement as sophisticated functional "features," there is no reason to believe that the switches (which are essentially specialized computers) cannot accommodate this functionality. The real problem is that the companies that manufacture and operate this equipment currently have no economic incentive or clear, specific legal requirement to include these functions as features in their developmental effort. If the needs of law enforcement agencies are accommodated during the developmental phase of new systems, features, and equipment, as is the case with other commercial services and features that are marketed to the public, adequate capabilities and access for electronic surveillance can be provided to law enforcement agencies without any adverse impact on the networks and without delaying the introduction of new commercial services and features.

Question. Can you describe several examples?

Answer. During the early 1980's, there was an explosive growth in the use of cellular telephones. The need to conduct electronic surveillance and pen register investigations within cellular systems became evident at an early stage. Unfortunately, the systems had been developed several years earlier and were being deployed rapidly. After unsatisfactory attempts to intercept cellular telephones on the radio frequency portion of the cellular system, law enforcement agencies sought the assistance of cellular providers in order to execute the court orders. Many cellular service providers (and there are literally hundreds of new companies for law enforcement agencies to deal with) were not aware of, or always responsive to, their legal obligation to assist law enforcement agencies with the execution of court orders. After a number of years, a number of technical solutions were eventually developed and deployed on a case-by-case basis (often with the government funding the system upgrade). The delayed deployment of these solutions led to an unknown (but we estimate significant) number of court orders not being executed, not being fully executed, or being delayed in their execution. Additionally, since these solutions were not considered in the development cycle of the cellular equipment and were of a "band aid," retrofit nature, in many instances the capacity range of some of these solutions was limited, which affected the number of simultaneous court orders that could be conducted, and in others their overall capability or functionality was limited.

Another example is call forwarding. When call forwarding was first introduced by telecommunications providers, the element that "forwarded" Or re-directed telephone calls was the central office switch. As such, even though a subject might forward his calls across the country, the content of the call itself still passed through the central office switch that served his telephone instrument. However, once forwarded, the subject's call did not appear in the local loop—law enforcement's traditional access point. Further, since no provision was made for lawful law enforcement electronic surveillance access during the development and deployment of call forwarding, service providers themselves were unable to afford law enforcement an effective means of acquiring such forwarded communications, even though they pass through their switches.

Question. I understand that the General Services Administration (GSA) was opposed several years ago to an earlier FBI proposal regarding this sage issue. Are they opposed to this latest version? Please explain what changes were made from the earlier version to the latest one?

Answer. As you are aware, the Administration's Digital Telephony legislative proposal, as well as an earlier legislative proposal formally transmitted to the 102nd Congress under the Bush Administration, deals with the issue of law enforcement's continued technical ability to conduct court-authorized electronic surveillances as advanced telecommunication technologies, services, and features are introduced into the nation's telecommunications networks. GSA is not a law enforcement agency and therefore has no expertise in the area of court-authorized electronic surveillances, nor does it have any particular expertise relative to any possible impact the incorporation of law enforcement's electronic surveillance requirements might have with regard to current or future networks, systems, features, or services. (By comparison, neither the FCC nor the National Institute of Standards and Technology (NIST), which also possesses telecommunications expertise, interposed any objection to the legislative proposal.) Unfortunately, in 1992, GSA comments were solicited by OMB in the context of an expedited legislative proposal clearance process, without GSA being privy to the numerous, lengthy, and in-depth legal and technical discussions and briefings which preceded the clearance process.

Consequently, although GSA's comments were considered along with those from other agencies within the Bush Administration, given the above, GSA's comments were evaluated accordingly. The important position was not GSA's but that of the Bush Administration. The Bush Administration determined that the only realistic way to effectively address the "digital telephony" problem was through a comprehensive legislative solution. Such a comprehensive legislative solution was formally transmitted to the 102nd Congress by the Bush Administration in September of 1992; however, time did not permit any action being taken on it.

In April, 1993, President Clinton directed that an interagency working group be established to examine, among other things, telecommunication technology trends and their impact on court-ordered electronic surveillances. After an in-depth eight month study, the Clinton Administration likewise determined that the only effective way to address the so-called "digital telephony" problem is through a comprehensive legislative solution; and a formal administration legislative proposal, entitled the "Digital Telephony and Communication Privacy Improvement Act of 1994," was transmitted to Congress on March 25, 1994. Fundamental to this decision was the Clinton Administration's belief, like that of the Bush Administration, that it would be unacceptable for the safety of the American public to be imperiled, the national security to be endangered, and effective law enforcement to be eroded through the diminishment or loss of this critical and essential tool of our nation's law enforcement and intelligence agencies.

The current legislative proposal is a significant improvement over the prior proposal, and includes a number of new and important provisions, many of which were developed after we received input from the telecommunications industry regarding the 1992 proposal. The current legislative proposal focuses on where the problems are—within the networks of common carriers. Hence, all other types of service providers (computer networks, PBX operators, etc.) have been eliminated from coverage. The time period for common carrier compliance has been doubled from 18 months to three years. The wording of the electronic surveillance requirements has been refined based on industry suggestions. A "systems security provision" has been added to reflect that any Premises/switch-based intercepts will only be initiated by designated common carrier personnel. The assistance of the FCC is included. Importantly, a provision for on-going "consultation" using industry standards bodies and other fora is established to ensure cost-effective compliance, and the Attorney General is authorized to reimburse common carriers for all reasonable costs directly associated with the modifications required to be performed in order for common carriers to comply with the Act, up to $500 million under the current proposal. Finally, the proposed legislation includes provisions that improve communications privacy protection for cordless telephones, certain radio-based data communications, and communications transmitted using certain privacy-enhancing modulation techniques.

Question. The telecommunications industry claims this legislation would go well beyond the status quo by allowing the FBI to be part of the front-end design process, where it has not been previously. How do you respond to their concerns?

Answer. The industry's claim is erroneous. The purpose and effect of the Administration's proposed legislation is to clarify and define the *existing* responsibilities of common carriers to provide the "technical assistance necessary to accomplish the interception." The proposed legislation does not require common carriers to design their systems in any one, particular way; and it certainly doesn't contemplate the FBI or any other law enforcement agency dictating network design. The legislative proposal simply requires that common carriers be able to respond to the long-standing generic electronic surveillance requirements of law enforcement and be able to meet their current legal responsibility to effectively "assist" law enforcement when served with a court order.

This legislation also does not propose that industry design systems with the ability to wiretap as the "design goal." Law enforcement is simply requiring common carriers to craft appropriate electronic surveillance solutions that interface with their networks' designs. Industry is in the best position to develop reasonable and cost-effective design solutions which accommodate, rather than frustrate, court orders for electronic surveillance and pen registers/trap and traces, and, at the same time, maintain the security and reliability of telecommunications networks.

Further, this legislation does not prohibit or impede the development or deployment of new telecommunications technologies. We are unaware of any authoritative industry statement that these requirements would significantly delay development or deployment of new technologies. Advanced technologies support a number of features that make systems more intelligent. The basic technology underpinning the introduction of advanced features and services, which often impedes electronic surveillance, likely will also offer solutions to these very problems.

Finally, law enforcement's.requirements will not dictate the course or pace of technology. However, with this legislation, our requirements will intentionally be included, rather than excluded, in the development of new technologies in much the same fashion that other legislation requires new technologies and products to take public safety into account and in much the same way that new commercial features and services are developed and deployed by telephone companies for purely economic gain. (For further information, see pgs. 54–55 of Director Freeh's statement for the record.)

Question. As telecommunications technology progresses will the FBI accidently acquire "content-based" information after only receiving authority to obtain "transactional" information (e.g., banking information) such as with a pen register, which only requires a grand jury subpoena—a lower standard to meet than a warrant issued frog a judge? How should the FBI address this problem? Is "content" information, obtained according to a subpoena, not a warrant, admissible in court? Should there be a heightened standard for content information, somewhere between "probable cause" and "reasonable suspicion"?

Answer. At the outset, the foregoing questions include a number of mistaken assumptions of fact, law, and investigative procedures. By clarifying these, a meaningful response best can be made. First, contrary to the false assertions of some in the privacy community, it should be made absolutely clear that the FBI and other law enforcement agencies do not focus investigative efforts on individuals who are not centrally involved in serious (felony) criminality. Further, United States Attorneys/District Attorneys do not authorize grand jury subpoenas or court orders, and courts do not issue court orders, where relevancy to a criminal investigation is not demonstrated. There are no "routine surveillances" of innocent people. Nor are court orders or subpoenas issued for irrelevant, noncriminal, or privileged information.

Second, under Federal law (18 U.S.C. 3121–27), a pen register lawfully acquires "numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. 3127(3). Such dialing information or "call setup information" is distinguished under law from call *content* which is dealt with under the Title III provisions (18 U.S.C. 2510–21) and from telephone *transactional records* which are dealt with under 18 U.S.C. 2701–11.

Third, use of pen registers by the FBI requires a *Federal court order* issued from a court of competent jurisdiction. Pen registers My not be used based upon a grand jury subpoena.

Fourth, if Title III content information is introduced in court, the provisions of Title III, including obtaining a Title 111 court order, must be followed in order to introduce such evidence. The use of pen registers to acquire the numbers dialed is expressly excluded from the treatment of interception of communications content under Title III. 18 U.S.C. 2511(h)(i).

Fifth, when the FBI acquires dialed numbers through the use of a pen register, these numbers mean nothing per se to the FBI. To determine the subscriber information pertaining to the party called (through the numbers dialed), the FBI bust then obtain a second form of legal process under 18 U.S.C. 2703 (a subpoena or court order) and serve it on the telephone company. The telephone company in such situations, of course, only possesses and hence only provides the *telephone subscriber or listing information* that identifies the called party (e.g., (202) 324–3000 is listed to FBIHQ, 10th and Penn. Ave., NW., Washington, DC.).

Sixth, assuming that the telephone number dialed by the criminal subject is determined to be (after subpoenaing the telephone company subscriber records) a banking or credit card institution, and assuming the FBI desires to examine the subject's financial records, then the FBI is legally obligated to obtain a third form of legal process and serve it on the institution, pursuant to the provisions of the Right to Financial Privacy Act, codified at 12 U.S.C. 3401–3422, especially 3413.

To the extent that dialing information (call setup information) tells something about criminal subjects and their activities, this has been the case since the first primitive "pen registers" were employed decades ago. Under the proposed legislation, law enforcement would acquire this dialing information *as it does today—no more no less.*

Although we are sensitive to legitimate privacy concerns, we have not received any information on this topic to suggest that any new laws are required or that current laws require amendment. For example, the notions propounded by Mr. Berman that either telephone transactional information under 18 U.S.C. 2703, or the call setup information (dialing information) obtained through pen registers under 18 U.S.C. 3121 et seq., or both, should only be available based upon a probable cause warrant is a radical departure from past law and jurisprudence and would cause the acquisition of electronic transactional information or records to be treated vastly differently than documentary transactional information and records. There simply is no legal or rational basis for according any type of telephone transactional information or records higher privacy protection than other documentary transactional information or records. As stated above, the dialing information obtained by a pen register always requires a court order, whereas telephone and documentary transactional information and records can be (and historically always have been) obtained through use of a subpoena.

Whereas the Government's legislative proposal simply seeks to maintain the legal/technical status quo, Mr. Berman and the DPSWG appear to be seeking a repeal of the pen register/trap and trace provisions enacted in the Electronic Communications Privacy Act of 1986.

It is particularly puzzling why some privacy rights spokespersons, under the guise of a "false transactional information scare," loudly advocate raising the legal bar to extreme heights for *law enforcement's* limited access to *information concerning criminal subscribers,* when *telephone companies* can afford broad access (and routinely sell, disclose, or exchange) much of the same type of information at issue here with the private sector *regarding all subscribers* with little or no legal constraint.

For a more complete statement regarding this issue,refer to pages 57–62 of the Director Freeh's statement submitted for the record.

Question. The telecommunications industry also is concerned that this legislation will harm their ability to compete with foreign competitors.

First, this legislation applies to all system and equipment used in the United States, not just American-made equipment and systems, is that correct?

Second, how do you respond to the industry's concern that their ability to compete for contracts in foreign countries will be harmed by this legislation?

Answer. First, the Administration's legislative proposal applies to "common carriers" who offer communications services which are *deployed* within the United States. The legislative proposal requires such common carriers to ensure that their *systems* have the capabilities and capacities to permit law enforcement to conduct court-authorized electronic surveillance. The proposed does not specifically address or apply to a single piece of telecommunications equipment but applies to a common carriers services overall.

Second, the proposed legislation does not prohibit U.S. manufacturers or service providers from developing or deploying telecommunications equipment or service for sale outside the United States which is different from that required pursuant to the proposed legislation. Domestically, the proposal would mean that all 2,000 common carriers would be competing on a "level playing field" because *all* common carriers would be required to meet the same requirements within the same compliance period.

Very importantly, other democratic governments also have basic law enforcement and security needs that are nearly identical to those in the United States. Consequently, because of undoubted demands for interception capabilities from law enforcement agencies in other democratic nations, United States manufacturers and providers are very likely to see increased demands from such foreign governments for this type of equipment and service, which will likely offer significant international sales opportunities. (See pages 55–56 of Director Freeh's statement submitted for the record for further information regarding this issue.)

Louis J. Freeh's Responses to Questions Submitted by Senator Leahy

Question 1. In your written statement, you refer to "numerous situations * * * where service providers * * * have been unable to provide assistance to law enforcement agencies," and cite the service provider's inexperience and lack of understanding of law enforcement requirements as the source of the problem. Was digital telephony or any new technology involved? In each situation, please identify the date, the service provider involved, and the specific nature of the problem. In addition, please describe for each situation whether law enforcement took any steps to compel cooperation by the service provider, and, if so, what those steps were and, if no steps were taken, the reason(s) why not. Finally, with respect to each situation, please indicate whether law enforcement and the service providers involved have been able to resolve the problem.

Answer. Generally speaking, most of the impediments encountered by law enforcement within the telecommunications networks are the result of advanced telecommunications technologies. These advanced technologies which support the deployment of new and emerging telecommunications systems, services, and features (e.g. cellular telephony, custom calling features, digital subscriber services) are largely *based on* digital telephony.

With regard to when, where, and the nature of the problems encountered, and whether any of the problems have been resolved, refer to the answers provided regarding questions 6, 7, and 9, below. Further information, as available, will be provided at a later date.

As stated below, the FBI has made numerous attempts to obtain the assistance of the telecommunications industry to resolve this problem *voluntarily*—but to no avail. Substantial efforts were made through the industry's Telephone Security Association (TSA), through meetings with Regional Bell Operating Company (RBOC) top executives, meetings with major manufacturer executives, Bellcore, and, for the last two years, through an industry-created ad hoc technical committee, which now meets under the auspices of the Alliance for Telecommunications Industry Solutions (ATIS).

To date, industry has failed to devise solutions to most of the problems, and the technical committee cannot guarantee the implementation of any solutions that may be developed. This critical circumstance was confirmed by ATIS Chairman P. Casimir Skrzyczak in his letter to the FBI dated March 1, 1994, which was furnished to the Subcommittees with Director Freeh's statement for the record.

To date, companies have been reluctant to undertake greater efforts to provide assistance absent a clear legal mandate, because they perceive that such assistance places them at a disadvantage when compared to other companies that simply refuse to expend developmental resources for law enforcement needs. The FBI has attempted to encourage service providers to voluntarily comply in different ways; for example, purchasing a known solution for the service provider.

Historically, law enforcement agencies have not taken any steps to compel cooperation by the service providers through legal action for several reasons. First, due to the time-critical nature of most investigations, the length of time needed to resolve a problem through litigation would not result in a satisfactory resolution. Second, litigation concerning such a problem would very likely compromise not just an investigation of a particular subject and his use of a subject telephone but potentially an entire investigation of a criminal group or organization. Three, there is no clear consensus that such legal action would result in the service providers being compelled to provide the needed assistance or held in contempt under the current law, where the provider is not technically capable of doing so at the time. The prevailing attitude expressed by industry representatives has been that the current statutory "assistance" requirement does not clearly extend to modifications of existing systems or to the development of new equipment or systems to support law enforcement electronic surveillance needs. Fourth, since the working relationships between law enforcement agencies and service providers have been generally good in the past, there has been a fear of damaging these relationships and ultimately impacting many other critical investigations negatively. In particular, within the last few years (and during rich time the survey was conducted), law enforcement has been attempting to have a dialog with telephone companies to obtain a firm and comprehensive commitment to meeting law enforcement's electronic surveillance requirements within a fixed and reasonable period of time. Seeking contempt of court or other such remedies during this time would fly in the face of this effort and undoubtedly would have been viewed as confrontational and counterproductive. For more detailed information, see pages 35–39 of Director Freeh's statement for the record.

Question 2. What steps have been taken by law enforcement to educate and inform inexperienced service providers?

Answer. When law enforcement agencies first become aware of a problem with the inexperience of some service providers, the problem was usually addressed by putting the service provider in contact with other service providers that had previous experience with the specific technological problem being addressed. Secondly, FBI TTAs frequently met with industry technical counterparts, advised them of the law, suggested technical solutions, and often identified or even funded modifications that would allow for at least some level of improvement. Such efforts, however, did not prevent the routine frustration of court orders, in whole or in part, and/or delays in executing court orders which often impaired investigations.

In 1991, the FBI next brought this problem to the attention of the Telephone Security Association (TSA), the industry association comprised of security office managers upon whom court orders are normally served and with whom arrangements are made to effect electronic surveillance court orders. However, TSA was unable to resolve the problems.

Later (in early 1992), the FBI along with other federal, state, and local law enforcement agencies, after consulting with industry representatives, developed and published a document entitled "Law Enforcement Requirements For The Surveillance of Electronic Communications." The purpose of this document was to provide telecommunications industry representatives with a generic set of requirements that can be referred to during the design of new systems. In addition to this document, in early 1992 the FBI began to meet on a regular basis with telecommunications industry representatives under the auspices of an industry-created Technical Committee to discuss these requirements. This committee, which was created by industry to avoid legislation, and which began as an ad hoc gathering, has since been chartered under the Alliance for Telecommunications Industry Solutions (ATIS) (formerly the ECSA) as the Electronic Communications Service Provider Committee (ECSPC). The ECSPC is made up of federal, state, and local law enforcement representatives, service providers, and manufacturers. Participation is voluntary and membership is open to all service providers and manufacturers. The ECSPC meets in committee on a quarterly basis with action teams meeting when necessary. The purpose of the ECSPC is to create a forum for dialog between law enforcement agencies and telecommunications industry representatives to discuss the legitimate needs of law enforcement with respect to new and emerging technologies.

Though helpful, this committee can only recommend solutions, assuming they are developed—it cannot dictate that any known solution be implemented. As important, there are over 2,000 common carriers and that number is increasing daily. As a practical matter, it is impossible for such a committee to bring about the deployment of needed solutions on a timely and comprehensive basis for over 2,000 common carriers. Legislation alone can assure this.

Question 3. The United States Telephone Association estimated that 1,200 digital switches in the U.S. are currently operational. Of the 919 wiretap orders and estimated 9,000 pen register orders authorized in 1992 for all federal, state, and local law enforcement agencies, were any such interception orders conducted on facilities using digital switches? If so, how many?

Answer. See Answer to No. 4 below.

Question 4. Up to this point, how any wiretap orders could not be executed because digital switches were used? For each nonexecuted order, please identify the date, the service provider involved, and the specific nature of the problem. In addition, please describe in each instance whether law enforcement took any steps to compel cooperation by the service provider, and, if so, what those steps were and, if no steps were taken, the reason(s) why not. Finally, with respect to each instance, please indicate whether law enforcement and the cellular providers involved have been able to resolve the problem.

Answer. It is certain that many of the estimated 919 wiretap orders and 9,000 pen register orders authorized within the U.S. during 1992 were carried out within facilities that use digital switches. For the most part, the local loop, which connects the customer to the central office, has been one of the few links within the network to remain relatively unchanged by the advent of digital switches, since the local loop is normally an analog link. This has allowed law enforcement agencies to continue to conduct court-ordered wiretaps on the local loop without regard to the type of switch being used. The digital switches that are being deployed today are capable of supporting sophisticated digital transmissions over the local loop; however, to date, these particular services have been sparsely deployed and have caused few problems for law enforcement agencies. However, the use of digital switches by service providers has led to the introduction of many new and sophisticated features and services that were not practical in an analog switching environment. It is the deployment of these new features and services, supported by digital technology, by the service providers that frequently has created problems for law enforcement agencies. As the features and services being deployed and offered by service providers have become more advanced, the communications and dialing information that law enforcement agencies attempt to intercept and acquire become less accessible in the local loop thus making it a less feasible access point, *and* effective central office access has not been developed by the telephone companies. Of course, in the near future when the many and diverse sophisticated digital-based services and features are deployed in the local loop, there will be substantially more problems.

Question 5. You have referred to an informal survey of federal, state, and local law enforcement agencies that uncovered 91 instances where interception orders could not be executed due to technology. Please detail how the survey was conducted.

Answer. The FBI relies on a Technical Advisor (TA) within each field office to coordinate the technical efforts necessary to execute court orders and other technical aspects of investigations. These TAs maintain *informal* technical liaison with many federal, state, and local law enforcement agencies within their field office area. The TAs within each office were asked to collect, through their contacts with other law enforcement agencies, information relating to *recent* technology-based problems that have impeded electronic surveillance/pen register/trap and trace efforts. This information was solicited and provided *on a confidential basis* in order to assure each agency that their ongoing investigations would not be hampered or compromised by the release of this information and in order to protect information regarding the law enforcement agencies' technical capabilities and inabilities. Additionally, this survey was not conducted in a rigorous, comprehensive, or in-depth fashion since participation was entirely voluntary and the information provided was generally limited in detail.

Nonetheless, the information obtained does clearly indicate that there are serious and widespread problems and serious implications regarding the frustration of court orders when telephone companies deploy technology without accommodating electronic surveillance requirements and without considering whether such deployment will, as a practical matter, prevent them from fully and effectively assisting law enforcement pursuant to the statutory "assistance provision" in the current law.

Not included in the tabulation were the numerous instances where court orders were not sought or had been "discouraged" due to these technological impediments. Since this survey was conducted, the FBI has become aware that technology-based problems have been encountered in many more instances.

Question 6. In 40 instances the cellular provider could not provide called number information or had insufficient capacity. For each instance, please identify the date, the service provider involved, and whether the problem was one of capability or capacity. In addition, please describe in each instance whether law enforcement took any steps to compel cooperation by the service provider, and, if so, what those steps were and, if no steps were taken, the reason(s) why not. Finally, with respect to each instance, please indicate whether law enforcement and the cellular providers involved have been able to resolve the problem.

Answer. See answer No. 9 below.

Question 7. You have cited 29 instances in which interception orders were impeded because of custom calling features. For each instance, please identify the date, the service provider involved, and whether the problem was one of capability or capacity. In addition, please describe in each instance whether law enforcement took any steps to compel cooperation by the service provider, and, if so, what those steps were and, if no steps were taken, the reason(s) why not. Finally, with respect to each instance, please indicate whether law enforcement and the cellular providers involved have been able to resolve the problem.

Answer. See answer No. 9 below.

Question 9. You have generally referred to the nature of the problem in 69 of the 91 instances in which interception orders could not be executed due to technology. what was the problem in the remaining 22 instances? For each of those 22 instances, please identify the date, the service provider involved, and the problem. In addition, please describe in each instance whether law enforcement took any steps to compel cooperation by the service provider, and, if so, what those steps were and, if no steps were taken, the reason(s) why not. Finally, with respect to each instance, please indicate whether law enforcement and the cellular providers involved have been able to resolve the problem.

Answer. The survey that is the source of these numbers, as indicated above, was conducted in an informal way, as a means of trying to determine the scope of the problem that existed at that time and how it was affecting law enforcement agencies. In order to encourage law enforcement agencies to candidly share information regarding the technological problems they were encountering, the survey was rather narrow in the scope of information sought. Hence, many of the details you have requested were not acquired in the survey. The various agencies were asked only to provide information (no level of detail specified) regarding court orders that were frustrated by technology-based problems.

Of the forty (40) instances of technological problems involving cellular providers that were identified, ten (10) instances resulted from insufficient capacity within the service providers' systems. However, the overall number of court orders that have been frustrated due to limited capacity within the cellular system is known to be much greater than this. It is known, for example, that a large number of requests for cellular-based electronic surveillance and pen register/trap and trace court orders have been discouraged in various localities because of the cellular capacity problem and were therefore never prepared for submission to a court. Although many of the cellular capacity problems have been addressed, some still remain. In addition, there remain many aspects (capability problems) where law enforcement requirements for electronic surveillance of cellular communications have yet to be addressed.

Twenty-nine (29) of the instances of technological problems reported through the survey were associated with custom calling features. Because service providers traditionally have refused law enforcement admittance to central office facilities or have discouraged law enforcement agencies from conducting interceptions from within their central office facilities, and because in the past adequate access could be obtained by law enforcement on the outside plant portion of the telecommunications network, most electronic surveillance/pen registers have been technically effected in the local loop. However, the deployment of calling features has created serious problems for law enforcement agencies and has resulted in the frustration of court orders. For example, abbreviated dialing features have allowed the subjects of interceptions to place calls from their phones by dialing a short sequence (e.g. No. 2) which is translated at the central office into a full 10 digit telephone number. There is currently no means for law enforcement to obtain these translations in real-time—nor have service providers themselves solved this problem at this time. Other calling features, such as call forwarding, similarly pose serious problems and frustrate court orders. Call forwarding, in many instances, is carried out by the service provider at the central office switch. The telephone companies' deployment of call forwarding permits subjects to utilize call forwarding to reroute their communications to a distant telephone number. In these cases, communications of interest to law enforcement are not accessible in the local loop. Further, telephone companies themselves have not devised solutions, to date, to capture these communications. Although we have not specifically tracked these problems, we know they remain, and we have no reason to believe that they have been resolved where they occurred since they were reported.

The remaining twenty-two (22) instances were in several major categories: Features (other than calling features) such as Voice Mail; central office-based digital subscriber lines (e.g. CENTREX); multiplexed digital transmission lines (e.g. T–1); service provider furnished encryption; fiber optic lines; and trap and trace inabilities on the part of the service provider. Although we have not specifically tracked these problems, we know these problems remain, and we have no reason to believe that they have been resolved where they occurred since they were reported.

One feature that was recently deployed by some service providers has already created problems for law enforcement agencies. "Voice Dialing" is a form of abbreviated dialing feature that allows a user to "dial" a phone number by speaking into the telephone. For example, a user might say "Call work" and thereby be connected to his work phone by the service provider who has equipment capable of recognizing and decoding his voice. Law enforcement agencies utilizing a pen register to acquire the dialing tones in order to obtain dialing information cannot capture this dialing information. Unless service providers devise a method of furnishing law enforcement agencies this information, many pen register court orders for dialing information will be frustrated.

Historically, law enforcement agencies have not taken any steps to compel cooperation by the service providers through legal action for several reasons. First, due to the time-critical nature of most investigations, the length of time needed to resolve a problem through such means would not result in satisfactory solutions. Second, litigation concerning such a problem would very likely compromise not just an investigation of a particular subject and his use of a subject telephone but potentially an entire investigation of a criminal group or organization. Third, there is no clear consensus that such legal action would result in the service providers being compelled to provide necessary assistance or held in contempt under the current law, where the provider is not technically capable of doing so at the time. The prevailing attitude expressed by industry representatives has been that the current statutory "assistance" requirement does not clearly extend to modifications of existing systems or to the development of new equipment or systems to support law enforcement electronic surveillance needs. Fourth, since the working relationships between law enforcement agencies and service providers have been generally good in the past, there has been a fear of damaging these relationships and ultimately impacting many other critical investigations negatively. In particular, within the last few years (and during which time the survey was conducted), law enforcement has been attempting to have a dialog with telephone companies to obtain a firm and comprehensive commitment to meeting law enforcement's electronic surveillance requirements within a fixed and reasonable period of time. Seeking contempt of court or other such remedies during this time undoubtedly would have been viewed as confrontational and would have been counterproductive.

Further, companies have been reluctant to undertake greater efforts to provide assistance because they perceive that such assistance places them at a disadvantage when compared to other companies that simply refuse to expend developmental resources for law enforcement needs. The FBI has attempted to encourage service providers to voluntarily comply in different ways: e.g., in some instances purchasing a known solution for the service provider.

Question 8. Please identify whether the FBI is aware of any technological solution(s) to provide wiretap capability for each custom calling telephone feature that impedes interception orders. what is the estimated cost per year of implementing the technological solution(s) that the FBI has identified for each custom calling feature?

Answer. The FBI, through its liaison with many foreign law enforcement agencies, has learned that a technological solution to many of the switch-based problems is under development in one of those countries. The foreign law enforcement agency in question has requested that the FBI not share the details or costs related to this effort. Aside from this constraint, further elaboration would involve classified information.

Question 10. Under the proposal, the Attorney General would be given authority to enforce the requirements. What is the mechanism the Attorney General will use to make accurate estimates of criminal activities requiring wiretaps as an investigative technique, so that industry will be given clear capacity guidelines? Is the FBI able to predict accurately the number of wiretaps that will be employed in the future? If so, has the FBI provided the telephone companies with those estimates and discussed wiretap capacity? What has been the result of those discussions?

Answer. The, Administration's legislative proposal contains a "consultation" provision (Section 3(g)) which encourages the Attorney General to consult with the FCC and the telecommunications industry to discuss details of the law enforcement requirements "related to capacity and cost-effective approaches." Pursuant to this provision, the Attorney General, through the FBI and other law enforcement representatives, will consult closely with industry so that industry will be able to develop appropriate and flexible deployment strategies for *their solutions* based, in part, upon historical interception activity as well as upon flexible components that accommodate broad "ranges of capacity." (See pages 5 and 6 of the legislative proposal's section-by-section analysis and page 47 of Director Freeh's statement for the record.) Approaches currently being discussed in the Electronic Communications Service Provider Committee, acting under the aegis of ATIS, will most likely allow for acceptable and compliant *ranges of intercept/pen register capacity* without the need to develop or be concerned with precise interception/pen register/trap and trace numbers.

Representative EDWARDS. Thank you, Mr. Freeh.

Senator LEAHY. I am going to yield to Senator Specter, but I would just make one point. None of us wants to impede the ability to go after kidnappers. I have been involved in kidnapping cases. I have been involved with missing persons cases. I have been involved in extortion cases. I have another district attorney beside me who is going to ask questions who has had far more experience than I.

I would just remind you of a survey done, a Time-CNN survey, that said 66 percent of the people thought privacy was more important than wiretapping capability by police. Now, obviously if it is your family involved, that may well change. But we do have some very serious privacy concerns in this country. I know you are dedicated to protecting privacy; we are dedicated to protecting privacy. But that is also one of the underlying questions of this whole thing.

Arlen?

STATEMENT OF HON. ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA

Senator SPECTER. Thank you very much, Mr. Chairman.

At the outset, I commend the chairmen of the Senate and House for convening this joint hearing. Coincidentally, Director Freeh, with your testimony today the Philadelphia Inquirer has a major story on "FBI Nets Stanfa In Mob Sweep," and the subheadline is "FBI's Rich Harvest Was a Tale of the Tape," which could not come at a more opportune time to underscore the kind of need of which you are testifying.

As Senator Leahy stated, I was district attorney of Philadelphia where we targeted the mob for a long period of time, so that I think there is a good bit of sympathy from the Congress on trying to accommodate law enforcement's interests.

I have just written a note to one of the chairmen asking if we might hear early from the telephone company on the technical problems—I have to excuse myself at about 11:45—to see what is involved there and perhaps have some insights from the civil liberties interests where there understandably a major concern. When you and I talked about this matter privately, we spent some substantial time on the civil liberties aspect.

I have long had a concern about wiretapping from the civil liberties point of view. Back in the mid to late 1960's I was the sole dissenter among Pennsylvania's 67 DA's on a a wiretapping issue. Therefore, I think the issue of need is fairly well established as to what you have testified to in results from today's headlines. But the technical questions, which Senator Leahy has put his finger on, are ones which I would like to hear. And I had made that suggestion, so I am going to be brief on this round as to you, hoping we can move into those other fields.

Thank you, Mr. Chairman.

Senator LEAHY. You do not want to talk about the Mafia up in your home town?

Senator SPECTER. No, I want to talk about the civil rights issues with some of the civil rights people if we can before I have to absent myself.

Senator LEAHY. Mr. Hyde?

Representative HYDE. Well, very briefly, Director Freeh, I do not have sufficient knowledge to ask a lot of interesting questions. I am here to listen and learn, but I can express my own view. The balance between the reasonable demands of privacy and the need of law enforcement to keep pace with the advances in technology is very important. I come down on the side of law enforcement, frankly, because it is easy to imagine one's own child being kidnapped and then demanding that everything be done immediately to find your child and to track the criminals.

Crime is certainly going to keep pace with technological advances, white-collar crime especially, and I think when one uses a telephone—I do not know how many people are naive to think that that is not something that people can listen to, especially in the mobile phones that you carry around. Involuntarily you hear other conversations, whether you want to or not, and most of them are not all that interesting. After 20 minutes I put them down. [Laughter.]

But I want to be helpful to make sure that you keep pace with the technology so that crimes of terrorism and serious felonies are not immune from the searching that you must do to solve them.

Thank you.

Senator LEAHY. Mr. Canady?

Representative CANADY. Thank you, Mr. Chairman.

I appreciate your testimony, and I would just like to ask you to expand a little bit on the efforts that the FBI has undertaken to date to resolve this situation with the telecommunications industry. I think all of us would agree that if this could be resolved without legislation, that would be desirable. It would be helpful, I think, for us to understand the steps that have been taken to date that bring us to this point where you believe that legislation is necessary.

Mr. FREEH. Surely. The discussion started in a very organized fashion approximately 4 years ago, obviously long before I came here. Meetings went on between representatives of law enforcement and the telecommunications industry for upwards of a year and beyond.

At a certain point, law enforcement was told by the industry that we were meeting with the wrong people, that we should have been meeting with a different group of their people. So we changed teams and started negotiating with a second group, the working group, which has been very beneficial. And I really think the Government should get some credit for having a dialog with the companies as we have. We have not introduced the bill. We have gotten some very important suggestions, some of which we have incorporated in our discussions.

But the problem is there are hundreds and hundreds of these companies, and to level the playing field by having everyone agree as to the requirements and timing is, in my view, a management impossibility, even though there is a lot of good faith on everybody's part.

If you were a judge supervising a multidistrict litigation with hundreds of parties, you would encourage them to meet together; you would require them to meet together; and they would, in fact, make progress from time to time. But there comes a point where there needs to be a process and there needs to be some mandated requirement, whether it be a motion deadline or a decision by the judge. But there has to be a point where a mandate is given, one, so everybody is on the same playing field, and, two, so everyone is looking to the same objective.

The companies have told us that they are not now putting into the software being designed the necessary access for us. So these switches which will be marketed and used in the next couple of years do not now have those things in there because they do not feel any compulsion to put them in there. And I do not blame them. If I were their lawyer advising them, I would tell them the same thing.

There has to be some requirement by law where the requirements of law enforcement will be designed and put into the package to maintain what we have now.

Representative CANADY. Thank you very much.

Senator LEAHY. First off, I do want to commend you for working with the industry. You, Mr. Kallstrom, and others have been over to see me and, I know, many, many other members on this. I know the great amount of time you and others have spent personally on it and in trying to work this out. I think that is what we all want to do.

But I have questions that raise red flags in my mind. The FBI's proposed requirements are written in pretty absolute terms. Companies are not excused just because they tried to help law enforcement. If they are unable to or fail to comply with the requirements, they could get up to a $10,000 per day fine. They could actually be closed down. That could happen even if there was a good-faith effort but an unsuccessful one.

Do you think that may be being just a tad bit too strict?

Mr. FREEH. As I said, with respect to the enforcement mechanisms, we have had a great history in this country between the Department of Justice and the telecommunications industry. I do not know of any occasion where the Government has made an application to hold a common carrier in contempt for noncompliance with an order, and there have been many instances of noncompliance.

I think you have to read that portion of the proposal as any district judge would read it, which is applying the rule of reason, the rule of good faith. I do not expect that the district court, unreviewed by a court of appeals, is going to shut down a phone company because they have made every possible good effort to comply and technologically have not been able to do so. And if the language needs some tinkering in that regard, that is fine. We are just looking to preserve access.

Senator LEAHY. You would want to be able to get real-time interception, no matter what feature is used by the subscriber. Does that set an industry-wide standard on cellular phones, for example? I understand the electronic serial numbers are now being changed by some criminals so the calls cannot be traced. Is that going to require some kind of clone-proof cellular phone?

Mr. FREEH. I think that it might. I think that there would be an industry standard with respect to software. I think that same software would also give the companies and us as their investigators the ability to apprehend and prosecute telecommunications fraud, which is several million dollars a day in terms of defrauding the companies. There is a flip side to this access which gives us the ability to prosecute people who are defrauding the companies out of millions of dollars.

Senator LEAHY. The proposed legislation applies only to common carriers, but as cable companies start offering telephone service, they might become a common carrier. Is that correct?

Mr. FREEH. That is correct. They are not included in the proposal.

Senator LEAHY. You say in your written testimony the proposal is limited to common carriers because that is where the vast amount of problems are. Some of the new technologies, such as personal communications services, would be exempted under your proposal. Does that make sense?

Mr. FREEH. Yes, there are parts of the industry—I am not so sure about the PCS's. I think the PBX's are exempted from the proposal. The personal communication systems, no, we would ask for access there. But you are correct that——

Senator LEAHY. Wouldn't the PBX exception be a big hole in the proposal? Why would they be exempted?

Mr. FREEH. Well, the computer companies would widen that hole. You are correct. We are excluding them, and for a couple of reasons: one, to narrow the impact and focus of the legislation. We could have incorporated it in there, as we did in the proposal 2 years ago, which was rejected out of hand. I think what we did in the interim is we made a concerted effort to narrow the impact of our focus and pick up where we think we will get the majority of criminal operatives. We are losing that, but that is a concession we are willing to make to narrow the package.

Senator LEAHY. A cable company or a radio dispatcher is not a common carrier, but they are developing new technologies where at least in some areas they may be able to provide telephone service. Does your proposal set up a competitive disadvantage? Is the phone company going to have to develop the software and have an industry-wide standard, but some of these other entities are going to be exempt? Will they be able to start moving ahead of the telephone companies in their own technology?

Mr. FREEH. Well, that is an argument, certainly, that the phone companies make. I am not sure of the validity of it, only because I do not have enough technological background. I do know and I do concede that there are portions of the industry that are not addressed in that legislation.

In a perfect world, they would be in there, but we want to narrow the focus of this so we can get the greatest support by the Congress and the committees, because the last time we were here, we were told specifically that it was too broad and it had to be narrowed and focused. So we picked out where we think we have the greatest vulnerability.

Senator LEAHY. You say this proposal would not expand law enforcement's authority to collect data on people, and yet if new technologies are used where we can dial up everything from a video movie to doing our banking over the phone, you are going to have access to a lot more data, just because the phone is being used.

Mr. FREEH. I do not want that access, and I am willing to concede that. What I want with respect to pen registers is the dialing information: telephone numbers which are being called, which I have now under pen register authority. As to the banking accounts and what movies somebody is ordering at Blockbuster, I do not want it, do not need it, and I am willing to have technological blocks with respect to that information, which I can get with subpoenas or another process. I do not want that in terms of my access, and that is not the transactional data that I need.

Senator LEAHY. See what absolute pussycats we are. Not a tough question among us.

Senator SPECTER. No pussycats here. I just want to hear the next witnesses. [Laughter.]

Mr. FREEH. Does that mean I can go?

Senator LEAHY. Those of us who are willing to stay here and work all day——

Senator SPECTER. I have a long line of tough questions for Director Freeh. I am just very regretful I cannot take the time to ask them.

Senator LEAHY. Feel free to go ahead.

Senator SPECTER. I will be doing a lot of work, not here, but later today.

Senator LEAHY. I do not question that. There are few people I have been with in the Congress who work harder than Arlen Specter.

I think, Director, you can understand from the nature of my questions and also from some of the conversations you and I have had privately, again, my concern. I will just reiterate it. As one who spent nearly a decade in law enforcement, I have a very strong feeling of wanting to help law enforcement in this area. I am also one who helped write our current wiretap law, trying to design it to take care of contingencies as technology changes.

I am also well aware of the fact that one of the areas where our country has an advantage over most other countries in the industrialized world is in the area of telecommunications. We have pushed the envelope as far as anybody ever thought you could in everything from our computers to the fact that a lot of our most effective industries today exist because they can move everything from vast amounts of data, blueprints, to phone conversations in matters of seconds across country and so forth.

The cellular phone industry has ballooned far beyond what anybody expected when it first came in, and technology has rapidly changed, unhindered really by anything other than the technological genius of the people doing it.

I do not want to suddenly put the brakes on everything because of law enforcement needs which may be taken care of by other ways. So that is a balance we are going to have work out.

I do applaud you and the FBI for the efforts that you have made, both with the Congress and others, to work this out. What I do not want to do is either privacy, which none of us would agree to do here, or intrude or inhibit what is probably one of the most remarkable parts of the industrial might of our country and our export ability.

Mr. FREEH. Senator, I applaud that, and I would like to think I believe in the Constitution as strongly and as deeply as everyone here. The Vice President asked me the same question when we were discussing this issue a couple of months ago, and I told him then and he certainly believes that nothing in this proposal should or will, in our view, impede the development of the superhighway of information. My point to him and my point to you is that we need and we will have a superhighway of information. But I think Americans want to have a cop on that highway, whether he is a Vermont State trooper or whether she is a Pennsylvania trooper or a California highway patrolman. We need that protection on that highway, and I think we can do it, and I do not see the privacy issues as being real issues once they are discussed.

Senator LEAHY. I would just leave with one thought. We have watched how the Internet, for example, has expanded and suddenly gone way beyond what anybody initially thought it would, but there were not a lot of governmental restrictions on it as it moved forward. Maybe it would have moved forward anyway.

I thank you very, very much. If there are no further questions, I appreciate your being here.

Mr. FREEH. Thank you, Mr. Chairman. If I might, just for the record, since I used to be a trial lawyer, I am going to respectfully submit to the committees and the respective chairmen written statements by Senator DeConcini and Chairman Glickman.

[The prepared statements of Senator DeConcini and Chairman Glickman follow:]

PREPARED STATEMENT OF SENATOR DENNIS DECONCINI

I appreciate the invitation of the committee to provide my views on the administration's proposed legislation on digital telephony. As I understand it, the purpose of the legislation is to require telephone companies who are using digital communications technology, or are planning to use such technology, to provide the Federal Bureau of Investigation with the means of intercepting such communications when such intercepts have been authorized by court order.

While I do have some misgivings with parts of the administration proposal, I do support, in principle, doing what is necessary to maintain the ability of the FBI to do wiretaps for law enforcement and intelligence purposes.

This is not an expansion of existing authority. But rather something that is needed to effectuate existing authority.

The case is amply made by the FBI that electronic surveillances have provided the key evidence in innumerable prosecutions of very serious crimes.

While mentioned less often, it is also clear that such surveillances have provided extraordinarily valuable foreign intelligence and counterintelligence. Digital technology poses the same problem for these kinds of surveillances as it does for law enforcement.

So, we must deal with it, and I am of the view that it cannot be done without legislation. There are too many telephone companies involved, and for this to succeed, the cooperation of all must be obtained.

I note the administration proposes to give these companies three years to comply with the FBI's needs and that the Government should reimburse these companies for the costs incurred. I think this is only fair.

But it is not clear to me how this is going to be paid for and at what cost. The proposal itself is open-ended in this regard and, in my view, this needs to be resolved at the outset.

I also find some of the provisions penalizing telephone companies who refuse to cooperate to be unnecessarily heavy-handed. If the Government pays the costs, I do not think it should take severe punitive measures to obtain their cooperation.

Having said all this, I return to my original proposition: the ability of the FBI to do wiretaps must be preserved. It is crucial to our ability to deal with terrorists, drug dealers, organized crime, espionage, and the other serious crimes which plague our society.

PREPARED STATEMENT OF REPRESENTATIVE DAN GLICKMAN

I appreciate the opportunity to offer some comments for the record of this hearing on the issue of digital telephony.

For several years, the Mouse Intelligence Committee has been advised of the increasing concern of the Federal Bureau of Investigation about its ability to continue to intercept communications in the face of rapid advances in telecommunications technology. This concern is shared by other elements of the intelligence community. Electronic surveillance has proven to be an extremely useful investigative tool, particularly in efforts to counter the activities of terrorists, reduce the flow of illegal narcotics, and conduct effective counterintelligence operations.

The advent of digital telecommunications technology and its increasing use threaten the utility of court-ordered electronic surveillance in the conduct of intelligence and law enforcement activities. I do not believe that Congress intended for statutes such as the Foreign Intelligence Surveillance Act and the Omnibus Crime Control and Safe Streets Act of 1968 to be rendered impotent by improvements in technology. A way must be found to ensure that properly approved wiretaps can be emplaced despite the development of ways to more quickly and efficiently route telephone calls.

I regret that the government and telecommunications providers were unable to reach an agreement through which access to modern telecommunications networks could be assured. A legislative response to this problem must now be crafted, and I urge that it be done so expeditiously.

While I am not endorsing a specific legislative proposal, I believe that it is clear that the current ability of law enforcement and intelligence agencies to conduct lawful electronic surveillance activities must be preserved. Technological impediments which hinder the execution of court-ordered wiretaps must be removed. This will not require an expansion of existing communications intercept authority, but rather the development of a means to ensure that the utilization of that authority is not frustrated by the advance of technology. The costs associated with implementing a technical solution must be allocated fairly, and the solution must apply uniformly throughout the telecommunications industry.

The intelligence community has made the Committee aware of many instances in which court-approved electronic surveillance has provided essential information unavailable through other ways. A lack of access to this type of information will hinder a number of essential governmental activities. I urge the subcommittees to take action to guarantee the continued availability of this important means of gathering intelligence and detecting criminal conduct.

Mr. FREEH. I would also like to, if I might, acknowledge for the record the presence here of Kevin Patrick from the International Association of Chiefs of Police; Bud Meeks from the National Sheriffs' Association; Lisa Harris from the National Association of Attorneys General; Deputy Chief Krupo from the Major City Chiefs; and Bill O'Malley will be a witness before the committee.

I thank you very much for your courtesies.

Senator LEAHY. Thank you very much. We are going to skip over just for the moment Mr. O'Malley. As I was once vice president of the National District Attorneys Association, I will assure Mr. O'Malley he is going to get to testify, but I do want to accommodate Senator Specter, and we will go to panel 3 first.

Thank you very much, Director.

Representative EDWARDS. May I submit for the record this letter from the International Chiefs of Police?

Senator LEAHY. Chairman Edwards has a letter from the International Chiefs of Police, and that will also be made part of the record.

Mr. Neel, you are to lead off on this.

PANEL CONSISTING OF ROY NEEL, PRESIDENT, U.S. TELEPHONE ASSOCIATION; AND JERRY BERMAN, EXECUTIVE DIRECTOR, ELECTRONIC FRONTIER FOUNDATION, ON BEHALF OF THE DIGITAL PRIVACY AND SECURITY WORKING GROUP, ACCOMPANIED BY RONALD L. PLESSER, PIPER & MARBURY

STATEMENT OF ROY NEEL

Mr. NEEL. Well, thank you, Mr. Chairman. I would be happy to do so. I appreciate this opportunity that you and the other chairman have extended. I would also like to echo what Congressman Hyde said about our disappointment at the retirement of Congressman Edwards. He will be missed.

I will summarize my remarks. You have my entire statement, and I will try to be brief to allow some time for questions.

It is not great fun to be here opposing a proposal that Director Freeh has put forth. He is certainly one of the major stars in this administration, and we are all pleased that he is there. But oppose it in its current form we must for a variety of reasons. I think the Director himself pointed out that there has been virtually no instance where a local telephone company has failed to cooperate with wiretap requests. Some, for technical reasons, have not been as smooth as perhaps both parties would like.

The FBI's own survey, which was obtained in a Freedom of Information request, showed, that there were "no instances in recent years" where there were problems here. In fact, Senator Specter's headline from the Inquirer I think is brilliant testimony to the fact that there has been clear cooperation between law enforcement and local telephone exchanges to pull off that success story.

It is extremely important that the public maintain confidence in the privacy of the national telephone system. You are going to hear more from Mr. Berman on that point, but just as Senator Leahy pointed out, the vast majority of Americans, telephone customers and everyone, remain concerned about the potential for a breakdown in privacy, and I think that is going to only increase.

The problem here is that this proposal does, in fact, dramatically broaden the ability of law enforcement to gain access to a much wider range of information about customers. I know the Director has noted that he does not want that information about what video rentals are being ordered and so on. But the fact is that, in part because certain providers are exempted and in part just because of technology and in part because of the FBI's expectation that they will need access to this so-called setup information that would be required under this proposal, it would be extremely difficult to ferret out the kinds of information that the Director says he does not want. And it is not easy to simply fix that.

One of the most disturbing aspects about this proposal is that it, in effect, forces the local telephone company to become the agent of law enforcement. That is quite a dramatic change in the relationship that we have had for all these decades in which we have had an arm's-length relationship between the local telephone company and law enforcement.

The scenario that Senator Leahy pointed out where you had a small telephone company in Vermont with five employees, the Director essentially said that a simple software fix would take care of any access problems and those employees could be at home asleep, we are not so sure that is the case. And, in fact, we believe that this proposal could very well force not only big telephone companies that do have substantial resources but also the very smallest telephone companies to maintain the kind of personnel capability that would allow law enforcement to get into a network when and where they wanted, real time, 24 hours a day.

Now, that says to me that just about any telephone company is going to have to have at least three people to maintain an around-the-clock access to that network at a risk of $10,000 a day fines.

I think we cannot shove the issue of cost under the table here. No one wants to put a price on law enforcement's ability to fight crime. Surely that is not your objective, and I do not think the telephone companies would want to do that as well. But an estimate of $300 to $500 million to implement this proposal, perhaps as much as a billion, as the Director pointed out, is in our estimation terribly low. We have information—and I think it has been widely discussed—that the cost of fixing only one aspect of this, which is the originating end of call forwarding, could be as much as $1.8 billion alone just in the short term. So it is important to know that this is not going to be a small drop in the bucket here.

It is also, I think, significant that this proposal would not appropriate any money for this purpose and that there is no authorization to spend money beyond 3 years. And I do not know anyone in this industry that believes that this problem can be fixed only during a 3-year window and then after that that it is a no-brainer. The fact of the matter is the lead time to develop technology that is typically deployed in the national telephone network is about 5 years or even longer. So it is hard to imagine that we could do this in the 3 years envisioned in this proposal and at the cost that it suggests.

Another very sensitive issue here is compensation. The Agency has now agreed that the local telephone company ought to be compensated for fixing these problems because, in fact, the only option there is that the local ratepayers would have to pay for these fixes. But the problem is where there have been cases where law enforcement is bound to pay these costs, getting those bills paid has been very difficult. And while a large telephone company might be able to absorb that, in fact, might even be able to write it off to avoid the public relations problem of suing law enforcement for compensation, a small company might have a very hard time meeting its balance sheet if it has to wait on a contested bill for a long period of time. And, in fact, this proposal suggests that law enforcement, the Justice Department, would decide what is a reasonable cost. So there would be no incentive really to pay these bills either on time or in the form they were presented. And I do believe that this would create a real hardship for smaller companies.

There are any number of cases where this has been an issue, and we would be happy to provide some of those.

There are so many other services that are going to be part of this network, and the Congress is already moving to open up these exchanges to competition. You want the local telephone company to face competition for all kinds of other providers. So we can expect a proliferation of such local providers getting into this business, private line services and so on. I think Senator Leahy asked the Director about the problem of narrowing the focus and exempting systems like PBX systems, motels and hotels, Internet was mentioned, Prodigy and so on. And the Director was very forthcoming on that, that it was narrowed and those kinds of services were exempted to avoid the kinds of problems that you might have in enacting this proposal—in other words, to take out of the picture the opposition from a number of technologies and companies and so on who might oppose this. And he said, of course, in a perfect world they would be in there.

The fact of the matter is that by exempting these other kinds of services, the ones we know now and the ones that we are certainly going to have in the future, we dramatically, I think, restrict the ability of law enforcement to go after the kinds of transactions, whether voice or data, that they will need to get at. It has been said by some in the administration I have seen quoted that criminals are stupid. But the fact of the matter is they are not so stupid that if they know they have a safe harbor to put a phone call in, to transact some sort of criminal business, if they know that it will not be tapped if they go over here and do it, then I am not so sure they are so stupid as to stay on the network where they know the conversation will be tapped.

Not only do we have all these current technologies and services, we are certain to have all kinds of new services that would be exempted from this. For instance, in addition to cable television that we have referred to, all the utility-provided services that are just expanding like wildfire, railroad communications, and the PCS equipment that has been referred to. Perhaps the Director believes that they will have access here, but the problem is the rest of the Congress is seeking to either deregulate or to make competitive these other kinds of services that would, in effect, make them not common carriers under the kind of scheme we are envisioning here. So there could be very large holes in the coverage of the Agencies' access to conversations and data. So I think that is not unimportant, and if there were to be such a plan put in place, it would clearly need to be universal in its coverage.

There has been reference to the effect on new technology here. I would certainly agree with the Director that this proposal would not stop the development of the information superhighway that you and our industry and certainly the administration want. The practical effect of this proposal would be a severe stifling of new technology and services and so on.

You have to remember that the telephone company does not just decide everything that is going to be developed, produced, manufactured, and marketed for a national telecommunications network. All of these new services we are talking about, most of them were, in fact, developed by entrepreneurs, small, medium, and large companies. So you have to consider the specter of anyone who would develop a new product, creating jobs and enhancing this network, having to make absolutely sure that this technology, this service, this product, is compatible with the Justice Department's technological requirements, which unfortunately are quite vague. It is difficult to manufacture to an ambiguous standard like this.

Turning the Justice Department into some sort of technology product certification office is not something I think that you would want, nor would we; moreover, they would have little incentive in accelerating the deployment of these technologies because of the various concerns the Agency has had.

I would not go so far as to say that it would seriously diminish our ability to export products, but it would clearly put a damper on the enthusiasm of entrepreneurs to develop products to deploy on this network if they are facing such severe sanctions if they just happen not to fit.

Now, we have talked a lot about the problems in this proposal. It is not unfair to ask what we would propose to fix this. The problem with the Agency's proposal here seems that there is some kind of magic wand that can be waved to solve this problem simply by decreeing that the local telephone industry shall fix this problem for everyone, even for providers that they cannot legally tap into, is a little unrealistic. A year ago, the General Services Administration pointed out that this proposal, as presented in an earlier form, was simply unnecessary.

We believe that what the Congress might want to do and, in fact, what the Agency should do is simply redouble its effort with the so-called Quantico Group. The FBI now cochairs this group and one of its major subgroups. I think that while the dialog has been going on for 4 years, this working group has only had about a year to work. So to essentially walk away from that experience, that cooperative industry-government activity, is a little bit like Michael Jordan being behind in the first quarter and saying, well, you know, we are just going to take the ball and leave the court.

The fact is you just redouble your efforts, work through these problems and go on. And I think it is not unfair to say that no matter what you do, even if this proposal were to become law, that does not fix the problems. You still have to have these kind of industry-government relationships to come up with the actual solutions. We are absolutely committed to that.

[Mr. Neel submitted the following:]

PREPARED STATEMENT OF ROY NEEL ON BEHALF OF THE U.S. TELEPHONE ASSOCIATION

Thank you, Mr. Chairman. I am Roy Neel, President of the United States Telephone Association (USTA).

USTA represents more than 1,100 local telephone companies ranging in size from the Regional Bell Operating Companies to small companies with fewer than 100 subscribers. Although many of the member companies of USTA have interests in a variety of businesses, USTA represents only their traditional telecommunications business. As a result, I will confine myself to sharing with the committee the perspective that local telephone companies have of this legislation.

I. WHAT IS THE "DIGITAL TELEPHONY PROBLEM?"

Let me begin by assuring the committee that USTA member companies always have, and always will, cooperate fully with the legitimate needs of law enforcement.

In the quarter century since the federal government first authorized court ordered wiretaps there have been tens of thousands of requests for assistance from local telephone exchange companies (LECs). In virtually every instance the local telephone company provided the appropriate law enforcement authority with the timely assistance it needed to effect the intercept.

USTA is aware of only a handful of instances in which there has been difficulty in providing assistance. These were caused by oversights in the original statute authorizing wiretapping which left certain issues, such as liability, unresolved. These oversights were quickly rectified, and since then there has been a long history of unblemished cooperation between LECs and law enforcement agencies.

The industry's cooperative spirit and commitment have been cited formally by the Bureau itself through the awarding of Certificates of Recognition from the Director, as well as through personal expressions of appreciation.

In fact, the Senate Committee Report accompanying the passage of the Electronic Communications Privacy Act (ECPA) refers to the statute's "technical assistance" provision as "a codification of the cooperative working relationship that exists between telephone companies and law enforcement."

Perhaps the best indication of the successful relationship we enjoy with law enforcement is that despite all the issues Director Freeh cited in his testimony, I am not aware of a single instance in which a wire line local telephone company has not been able to effect a lawful intercept due to complications related to advancements in technology.

Indeed, *The New York Times* of March 1, 1994, reports that documents obtained through the Freedom of Information Act indicate that a survey of several FBI offices found "no instances in recent years in which FBI agents had encountered any technology-based problems in conducting wiretaps."

At least one USTA member, Ameritech, which has taken a leadership role in several of the technical cooperative committees that have been formed to assist law enforcement, requested more than a year ago that the Bureau provide it with information on the number of "held orders" within their region. Not a single held order has been identified.

Perhaps this is why the federal government's own General Services Administration critiqued an FBI legislative proposal, similar to the current one in most major respects, as "unnecessary" and warned that it could "hurt the nation's competitiveness * * * and posed a possible danger to national security." (NYT 1/15/93)

Of course, the fact that there has not been a documented need for legislation to address a current problem regarding court-ordered surveillance does not mean that future concerns should not be anticipated and accommodated. Members of the local exchange industry are committed to continue and, if necessary, escalate their work with the various law enforcement agencies to address legitimate needs before they arise.

In 1992 the FBI first floated draft legislation which, while not attracting a congressional sponsor, did attract the interest of the telecommunications industry. Together we formed the Quantico Joint Government Industry Group which grew into a "Technical Committee" charged with the following:

- Developing a process for incorporating law enforcement's needs into future industry technological standards;
- Developing technical capabilities and procedures to permit continued interception by law enforcement of communications that use transition technologies; and
- Monitoring and tracking the timeliness of the industry's response to law enforcement requests. The committee's goal is "zero-held intercepts."

Through mutual commitment, the Technical Committee has now grown into a formal and permanent forum called the Electronic Communications Service Provider Committee (ECSPC). This committee is co-chaired by law enforcement and industry representatives. The commitment of the local exchange industry to this effort is evidenced by the fact that we have supported committee activities with funding of more than a half million dollars over and above the expenses of our personnel to assist the committee.

In short, Mr. Chairman, it is evident that the local exchange industry always has been and always will be committed to assisting law enforcement in addressing its interception needs. We believe that by building on this environment of cooperation, we can best serve the needs of all of the interested parties who use the public communications network.

We further believe that the proposed legislation ignores the historical relationship we have enjoyed with law enforcement. It is a punitive approach with unjustifiably harsh penalty provisions. It also forces local exchange carriers to become, in effect, agents of the law enforcement community, rather than maintaining the more appropriate arms-length relationship between common carriers and law enforcement.

II. HOW CAN LAW ENFORCEMENT GET BROADER AUTHORITY TO WIRETAP?

Naturally, we do not expect law enforcement to rely only on the good graces of the providers of communications services to fulfill their needs for lawful intercepts. However, when one looks at the current statute under which the cooperative spirit has grown, it is frankly hard to see how it could be usefully enhanced.

As I stated earlier, the original Omnibus Crime Control and Safe Streets Act of 1968 which authorized court-ordered wiretapping and which the FBI actively sought, was technically flawed and needed correction. Congress therefore amended the law on July 29, 1970. One of the amendments to the original law spoke specifically to the degree of cooperation that law enforcement had a right to expect from telephone companies. That amendment stated the following:

> An order authorizing the interception of a wire or oral communications under this chapter *shall* upon request of the applicant, *direct that a communication common carrier, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities and technical assistance necessary to accomplish the interception* unobtrusively and with a minimum of interference with the services that such communications are to be intercepted.

Virtually identical language appears in the Foreign Intelligence Surveillance Act of 1978 and the Electronic Communications Privacy Act of 1986 which also covers pen registers and trap and trace devices.

It is hard to imagine statutory language that more fully mandates cooperation with any possible needs law enforcement may have. The statute specifically says that a communication common carrier, landlord, custodian or *other person* shall furnish *forthwith all information facilities and technical assistance* necessary to accomplish the interception."

These statutes, together with the positive attitude we have cultivated over the past quarter century and with our intensive ongoing technical assistance, should be enough to assure that law enforcement maintains and enhances its ability to carry out legitimate surveillance activities.

III. IF THERE IS A NEED FOR FURTHER LEGISLATION, WHAT SHOULD BE ITS GUIDING PRINCIPLES?

Let me be clear about the position of the local exchange industry. We do not believe that a case has been made that legislation of the sort proposed by the FBI is warranted or wise at this time. However, we also recognize that the magnitude of this issue demands that this committee carefully and fully examine this issue and that law enforcement's needs are accommodated. In a continued vein of cooperation, we offer the following principles that we believe should guide the committee's deliberations.

A. All communications providers and networks should be required to assist the law enforcement community efforts to conduct lawful electronic surveillance

In the briefing materials that the FBI is widely circulating, the Bureau makes the following point:

> In 1970, the telephone industry was monolithic, and the part of the telecommunications network where the government effected electronic surveillance was relatively uncomplicated. Since that time, with the break up of AT&T through divestiture, the entry of numerous new communications providers in the marketplace and the introduction of many new technologies, services and features, the telecommunications networks have become more varied, advanced and complicated.

We could not agree more. In fact, the explosion of providers of various telecommunications services and networks is just beginning. Both Houses of Congress are currently considering legislation that will further stimulate the divergence of the telecommunications marketplace.

In the face of this developing multiplicity of communications providers, and in a legislative proposal attempting to address future technological developments, it is curious that the Bureau's bill narrows its focus only to common carriers. Private carriers, shared networks, PBX's, and computer networks—including the Internet—are all carved out of this bill.

If we assume, as the FBI assures us, that most criminals are stupid, then it would seem that we should be able to catch them without resorting to the FBI's proposal. If, however, we are to assume that we are dealing with criminals with even a modicum of intelligence, it would seem obvious that they would simply choose to communicate over, to quote the Bureau, "the many new technologies, services, features (and) networks" that are not covered by this bill. And, remember, the Bureau itself has acknowledged that these networks are growing rapidly.

Moreover, the existence of multiple providers of telecommunications also means that the government must select the entity that has access to a communication at the point where it can be identified and accessed. This may be before it enters or after it leaves the common carrier network. However, the bill places all of the requirements on the common carrier alone. Does this mean that we as the common carrier must now go and effect the tap on someone else's network for law enforcement? And if we do not, are we subject to fines of $10,000 per instance per day and to the ultimate fine—having our service shut down? And what happens to telephone subscribers in that event? Incredible as it may seem, that is what the language of the proposed legislation would provide.

USTA believes that an essential feature of any proposal, legislative or otherwise, must cover all available communications modalities available to criminals in order to prevent circumvention. This is particularly appropriate with a proposal, such as the current one, which carries such a potentially large price tag for carriers entering a competitive era.

B. Public confidence in the public network must be maintained

One of the hallmarks in the security of our nation's telecommunications system is the ability to provide secure communications. Confidence in your conversations is more than a core element of the privacy that we have come to expect; it is an essential feature of maintaining the nation's economic foundation.

The proposed legislation calls for common carriers to build the capability into their networks to hold and receive at all times sufficient capacity to "execute expeditiously and simultaneously * * * all court orders and lawful authorizations for the interception of wire and electronic communications and the acquisition of call setup information" to be delivered "unobtrusively" to any remote location specified by any federal state or local government entity "authorized by law to conduct electronic surveillance."

In describing its proposal, the FBI strongly asserts that it is not seeking expanded authority. We must, with all due respect, disagree. We believe that this is a level of surveillance capability unprecedented in terms of immediacy, breadth of application or capability for routine surveillance of individual citizens.

Furthermore, the increasing use of telecommunications in all aspects of life as we move into the "information age" means that a substantial behavioral profile can be developed with great precision from "call set-up" information. And, although the discussion of this issue sometimes gets fuzzy, we need to remember that, under this proposed legislation, call set-up information does not necessarily require the issuance of a court order based on probable cause.

A dramatic illustration of the primacy that our citizens place on their privacy is the fact that while the media is rife with stories about violent crime, a poll conducted two weeks ago by the Yankelovich Partners and reported in *Time Magazine* March 14 found that "two-thirds of Americans said that it was more important to protect privacy of phone calls than to preserve the ability of the police to conduct wiretaps."

Like any citizen, I am troubled by the implications of the IRS or local law enforcement gaining access to an extensive personal profile of me without any court order. But I will leave it to others on the panel to develop that issue.

From a purely business perspective, there also are troublesome issues involved here that transcend the concerns of telephone companies. Just last Congress, Chairman Brooks held a hearing on the issue of corporate surveillance. He pointed out that American corporations had billions of dollars at risk due to corporate espionage.

While that hearing focused more directly on the "encryption" issue which is not considered in this specific legislative proposal, I further suggest that in the public's mind these issues will merge. And I suggest further that perception and public confidence in the nation's telecommunications network are very much at issue here.

If the public becomes skittish about using the public network for fear either that it is full of "back doors" designed so that the FBI can more easily tap into it, or that their local sheriff will be developing a dossier on them based on call set-up information, that fear will translate into reduced use of the system. The result will be the loss of billions of dollars in potential revenue, and along with that many of the jobs, the taxes, and the benefits that we anticipate from the information age.

C. Rate payers should not be required to pay for law enforcement's upgrades

This is, of course, the old bottom line issue of who pays for the law enforcement's system. In this respect USTA acknowledges that there has been some progress made with the Bureau. The Bureau has moved away from its original position that the telephone companies absorb these costs as a "cost of business." It is now rightfully acknowledged that such a procedure would simply mean that costs are passed on to telephone customers in the form of rate increases.

We now seem to agree on the essential premise that law enforcement itself should pay for the cost of system alterations. Law enforcement is a public good; therefore, funds for these alterations should come from general tax revenues. But, heavy telephone users do not benefit from law enforcement more than other users and should not bear a disproportionate share of the costs of law enforcement.

Even with that basic premise agreed to, the current legislative proposal makes several unrealistic assumptions that would, in the end, cause telephone rate payers to absorb substantial rate shock, particularly in the "out years."

First we have to have some idea of how much these system upgrades will cost. The Bureau has expressed significant interest in the issue of call forwarding. Preliminary USTA estimates are that the software upgrades alone necessary to capture the needed information at the originating end of these calls would cost between $180 million and $1.8 billion.

In addition, new equipment and software would have to be developed to assure that carriers have the "ability to intercept the content of communications," particularly in the approximately 1,200 ISDN switches deployed throughout the nation. Estimated costs here are approximately $450 million.

This does not even anticipate the costs associated with newer technologies such as photonics and asynchronous transfer mode. USTA's technical disciplines department does not even have rough cost estimates on these items, but they will certainly be significant.

The point here is not that we cannot make the adjustments law enforcement says it needs. In fact, we can. However, there will be costs involved—costs that will likely go far beyond the Bureau's estimates both in number of dollars and number of years.

Since we have agreed that the general population, not just telephone subscribers, should pay for whatever upgrades law enforcement requires, the artificial caps, such as the three-year maximum period for which the government will cover expenses, must be eliminated. Similarly, we strongly question law enforcement's technical ability to be the judge of what constitutes "reasonable and cost-effective charges directly associated with modifications required to assure common carrier compliance."

Surely decisions about what constitutes "reasonable and cost effective" and "directly associated" cannot be made solely by the entity footing the bill.

D. The information age cannot be delayed

I have already referred to the legislation advocated by the Administration, designed to hasten the advent of the "information superhighway." The priority of this effort should not be underestimated. The prospect for making the best teachers and educational materials in the nation available to every child regardless of geographical location or economic means is close at hand. The ability, through telemedicine, to enable the world's best doctors to consult in real time for patients in distant locations, is now practical. The ability to diversify our economy from the central cities, and, in doing so, substantially reduce environmental pollution and save energy is realistic.

But all of these advances are the outgrowth of the speedy deployment of a modern information infrastructure. This bill calls into question the priority of this effort and creates an enormous speed bump in the information superhighway.

This legislation would make the Attorney General the arbiter of whatever technologies and equipment can be deployed in the public telecommunications network. Presumably this is necessary to assure that new systems, or at least the new systems deployed by the common carriers, will be susceptible to ready interception and real time delivery of desired information to remote areas.

While we recognize the priority of law enforcement's needs, we also recognize that it is not the only priority. Our nation cannot be held hostage to inexpert analysis of telecommunications technology as we move to the information age. We strongly suggest that the system of cooperation and communication that we have always had and which we have enhanced dramatically in just the past few years is the far more preferable approach.

IV. A LESS DRACONIAN APPROACH TO THE PROPOSED BILL IS BETTER PUBLIC POLICY

Mr. Chairman, we understand the FBI's fears about the future of telecommunications. We have a considerable fear about the future of the telecommunications business ourselves. But the answer to those fears is certainly not the bill that has been proposed, and may it not be legislative at all.

The proposed bill is an overly broad bill. It does not cover all of the technologies and systems that should be covered by any rules that are put in place. It makes unreasonable and perhaps impossible demands on those it does cover. It is unnecessarily punitive in nature. It fails to account for the need to address issues other than law enforcement needs, and it is economically unfair and impractical.

USTA and its member companies will always stand ready to assist law enforcement in the performance of its legitimate functions, and we stand ready to assist this committee in any process that it sees as appropriate to assure that law enforcement needs are anticipated and accounted for.

And, Mr. Chairman, you have my personal assurance that I will assist you in any way you deem appropriate in resolving any outstanding issues.

U.S. TELEPHONE ASSOCIATION,
April 27, 1994.

Hon. PATRICK J. LEAHY,
Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR SENATOR LEAHY: Attached are USTA's responses to the questions you posed in your letter of March 23, 1994. Those related to specifics of wiretap events have proven difficult to answer, because USTA historically has not been directly involved in wiretap activity. Such operations have been conducted directly between the affected law enforcement agencies and the individual companies providing technical assistance. However, based on discussions with member companies, we have answered your questions as thoroughly as possible.

USTA and a number of its member companies have supported, and currently support, the deliberations of the Electronic Communications Service Provider (ECSP) Committee, which is addressing wiretap technological issues from an interindustry perspective in conjunction with law enforcement representatives.

This broad, interindustry approach is essential to the development of standards that will support the ubiquity of surveillance capability upon which the FBI depends. Contrary to the apparent expectations of the FBI, this is not a one-time activity. Because technology will continue to evolve, there will be a continuing need to develop standards for new technologies and new applications. This necessarily will involve interaction between representatives of the affected industries and of law enforcement agencies to assess the trade-offs that must be resolved between the costs and benefits of specific solutions. USTA and its members remain committed to this important activity.

USTA believes the currently proposed legislation is flawed. However, we are continuing an industry effort to help develop proposals which might be beneficial to reassuring the FBI of wiretap capabilities while also retaining a balance with other objectives such as customers' concerns for privacy of communications, availability of network advancements and costs to deploy new technologies.

I look forward to working with you and your Committee on this important issue.

Sincerely yours,

ROY NEEL,
President and CEO.

ROY NEEL'S RESPONSES TO QUESTIONS SUBMITTED BY SENATOR LEAHY

Question 1. Current statutes applicable to wiretaps, pen registers and trap-and-trace devices already require service providers to furnish "forthwith" all information, facilities and technical assistance necessary to accomplish the installation of the equipment to carry out the court order. Failure to comply could result in a contempt proceeding against the service provider. Is the threat of a contempt proceeding effective in compelling telephone companies to cooperate with law enforcement agencies in implementing interception orders? What penalties would be effective?

Answer. The current law applicable to wiretaps, pen registers and trap-and-trace devices is effective to assure compliance. Telephone companies strive to meet all requests within the time specified, with professionalism, and in cooperation with law enforcement officials. The telephone industry takes very seriously its responsibility to respond to law enforcement requirements. Given the long history of cooperation between our industry and law enforcement we believe additional penalties are unnecessary.

Question 2. Do you interpret the "technical assistance necessary" language of Section 251(4) of Title 18, to require service providers to take affirmative steps to develop technical solutions to accommodate or effectuate a court's electronic surveillance order?

Answer. The Congressional Committee report on Section 251 states that it "* * * is a codification of the cooperative working relationship that exists between telephone companies and law enforcement officials." The report describes that relationship as follows: "Telephone companies have, as a matter of practice, provided information and technical assistance to law enforcement officials in connection with lawfully authorized wiretaps." Therefore, it is useful to examine the nature of the assistance provided today in order to interpret this statutory term. "Technical assistance" most often involves work by service providers that is operational in nature rather than technological. But telephone companies also have assisted in developing solutions to technological problems that have arisen when implementing particular wiretap orders. This assistance has involved such matters as a lack of working lines, malfunctioning lines, network equipment congestion (in the feeder plant) and lines with special features, such as Voice Mail. In practice, service providers and law enforcement agencies work cooperatively to find ways to implement and effect court orders.

Question 3. Can the same technology used by telephone companies to isolate particular lines for billing and maintenance purposes also be used to support a wiretap capability even as telecommunications networks become more advanced and digital transmissions are used from end-to-end? If not, what options are there for intercepting all communications associated with a specific digital line at a point or points remote from the customer's premises? Are options being studied or developed to permit for isolation of a particular line to a subscriber?

Answer. Telecommunications manufacturers and software vendors are in the best position to address the use of billing and maintenance systems to effectuate wiretaps. FBI requirements are different from a telephone company's record keeping needs, making it difficult to use current billing and maintenance technology for law enforcement purposes. For example, when fixing a customer's line, a telephone company's work need not be transparent to the customer.

For ISDN lines, existing test equipment can do much of what is needed to accommodate the needs of law enforcement agencies to access specific lines at a point or points remote from the customer's premises. Additional options have been studied in the ECSP Committee (under the auspices of the Alliance for Telecommunications Industry Solutions) to address ISDN and Digital Loop Carrier. ECSP is writing generic requirements for telecommunications equipment so that vendors can develop capabilities to gather data at the service provider's switch. At the switch, a particular customer line could be selected and monitored using this capability.

Question 4. You estimated in your written testimony that 1200 digital switches in the U.S. are currently operational. Have any interception orders been conducted on facilities using these digital switches? If so, how many?

Answer. Interception orders are conducted on lines that are connected to digital switches. The number of wiretaps on such facilities is not tracked by switch type because interception orders typically are executed in such a way that the switch type is not relevant.

Question 5. The FBI and telecommunications industry representatives have been meeting over the past couple of years to address law enforcement needs for continued wiretap capability. The FBI does not believe that this process is adequate to insure that any technological solutions to solve wiretapping problems will be implemented. Is the FBI correct in their evaluation of how well this Committee can work, even if all the participants operate in good faith with the best intentions?

Answer. There may be some confusion as to the role of the ECSP joint industry/law enforcement committee. Its purpose is to develop technical proposals for how law enforcement requirements can be met. The ECSP is making excellent progress in achieving those objectives. It was not intended, nor does it attempt, to address implementation commitments by individual companies.

Question 6. The FBI seeks to have industry, with its more thorough knowledge of the operations of telecommunications systems, develop the means to implement interception orders. The alternative would be for law enforcement agents to effectuate interceptions using their own equipment in complex, sensitive networks. This carries the risk of disrupting service. Is it better to have the telephone companies work with networks, switches and switch software, since they have the expertise, and provide the capability for wiretapping?

Answer. It is better to have the industry working with the customer (*i.e.,* law enforcement agencies) to develop technical requirements. Service providers have more expertise with networks, switches, and software and can work with equipment and software vendors to create solutions in a consistent and standard way. This approach reduces the risk of disrupting service.

Question 7. Could features designed to facilitate law enforcement access to communications increase vulnerability to unauthorized interception?

Answer. It is difficult to predict how features designed into networks to facilitate law enforcement activities will affect the reliability of the network. However, features designed to facilitate law enforcement access to communications could well increase the vulnerability to unauthorized interceptions. This is because the more opportunity provided to any group to gain access, the more opportunity for the unauthorized to gain access. On the operations side, the responsibility for monitoring and upgrading the capability and using the technology effectively will fall to the service provider. Besides the surveillance capability itself, a secure operational support system may be required to manage the process. This is one reason why interindustry standards must be set and followed regardless of what other issues may be addressed in legislation.

Question 8. If law enforcement's requirements had to be designed into every new piece of telecommunications equipment or new system, would this have any effect on how quickly American manufacturers could bring their products onto the market?

Answer. It could significantly slow development and implementation of new technologies/services. Law enforcement requirements would be another necessary consideration before designing and ultimately building a product. It would greatly affect manufacturers that have not built in these requirements, as existing equipment would become obsolete or need major upgrades.

Question 9. If designing and developing wiretap friendly telecommunications equipment and systems slowed down advances in U.S. technology, would this effect the competitiveness of U.S. industry in the global market?

Answer. A slowing of the development of domestic technology, such as described in response to question 8, would generally impair international competitiveness. After a piece of technology is developed domestically, the answer to this question then depends upon countries' policies regarding wiretaps, etc. If there is sufficient demand in other countries for these capabilities within their communications network, then vendors would have an opportunity to serve those markets as-well. If there is insufficient demand in other countries, then the costs to provide such capability in equipment of American manufacture could reduce its competitiveness in global markets.

Question 10. Do you have a sense of whether American telecommunications equipment and systems will be more marketable overseas to foreign governments and foreign customers if these products incorporate law enforcement's requirements and are wiretap friendly?

Answer. See the response to Question 9.

Question 11. Existing law requires the government to pay for all "reasonable expenses incurred" by a service provider in assisting the government to execute wiretap orders. Under the FBI's proposal, the scope of industry's assistance would be expanded to include designing future telecommunications systems and equipment to comply with law enforcement's wiretapping requirements. What is your estimate of how much these design requirements would cost taxpayers in the future?

Answer. In order to answer this question on costs with any precision, one needs to know the technical impacts of law enforcement requirements in a number of areas, including present capacity demands, future capacity demands, coverage areas, amount and format of information, delivery mechanisms (store, leased line, dial-up), security measures, functionality, and features. The ECSP committee has made progress in writing generic requirements to guide vendor development. One would need estimates from the vendors about the cost of building these capabilities. We believe the cost could exceed a billion dollars. In one sense, these costs would continue into the future indefinitely, since each new system developed in the future would have to be designed and manufactured to meet these additional requirements.

Question 12. As personal communications services and networks (PCS/PCN) are developed, will the industry be able to isolate and intercept at a particular point remote from the customer, all communications associated with a specific customer number? What points will that be? If not, is that a capability being developed?

Answer. While the provision for PCS/PCN services generally lies outside the scope of USTA's member local exchange carriers, it is our understanding that a significant amount of work concerning PCS/PCN is being conducted in industry standards bodies. The ECSP Committee will be presenting contributions to several U.S. standards groups in the next few months regarding PCS. These contributions describe law enforcement's requirements for the lawfully-authorized interception of call setup information and call content, and discuss a concept for meeting these requirements in a PCS environment. (Last week, the ECSP Committee presented to one U.S. standards body a contribution regarding the requirements and capabilities sought in PCS for wiretaps.)

Question 13. Some of the noncommon carrier companies going into the wireless and PCS technologies will be direct competitors of the telephone companies, who would be subject to the FBI's requirements in the proposal. Would this have any effect on the ability of telephone companies to compete with these new technologies?

Answer. The same requirement to assist with wiretaps needs to be established for all entities that provide telecommunications services. All service providers (including noncommon carriers) must be required to work, support, implement, and comply with law enforcement requirements. In that way, broad compliance can be achieved and the competitive impacts will be lessened. To do otherwise would put common carriers at a disadvantage, but even more importantly, without the full ubiquity of law enforcement capabilities, there would be services where law enforcement would not have access to the call setup and call content information. People intending to violate the law can be expected to find the service providers for which law enforcement lacks wiretap capabilities and exploit the situation.

A related concern is whether it is cost effective to insist that each and every new telecommunications capability used on common carrier networks meet the proposed requirements. Some of these new capabilities would be deployed only for limited and special applications. They are not likely to be used by the typical targets of wiretap orders, and so one must question whether it makes sense to spend significant amounts of time and money on ensuring they meet the proposed requirements.

Question 14. The FBI has cited 91 instances in which law enforcement agencies could not execute interception orders due to technology. Forty instances apparently involved cellular providers, but in 29 instances, special calling features were the problem. The problem or problems in 22 instances were not identified by the FBI. Is your association or any members of your association aware of what the problem or problems were in the 22 instances referred to above? In addition, could you describe what, if anything telephone companies have done to assist law enforcement in executing interception orders involving special calling features that may thwart interception orders?

Answer. USTA has not had a direct involvement in handling wiretap orders, as this activity is conducted between the relevant law enforcement agency and the telephone operating company serving the surveillance target. Accordingly, we cannot respond at this time to the particulars of the alleged 29 instances involving special calling features. We do know that the ECSP Committee, in which USTA and its member companies participate, is working to identify circumstances that may interfere with wiretap capabilities and to develop standards for solutions. We also are aware of instances where a member company has facilitated wiretaps on special calling features for law enforcement agencies, including real-time voice mail interceptions.

Question 15. The FBI has conservatively estimated that, over the last decade, several hundred electronic surveillance, pen register and tap-and-trace orders have been frustrated, in whole or in part, by various technological impediments. Is your association or any member of your association aware of what the technological impediments are that would frustrate this number of interception orders? Please describe those impediments and what efforts, if any, the industry has taken with respect to overcome each impediment and assist law enforcement.

Answer. For the reason stated above, USTA is not in possession of specific particulars on wiretap events. The appropriate body to assess impediments encountered due to various technologies is the ECSP Committee, which is supported by a number of relevant industries in addition to USTA and its member companies.

Senator LEAHY. Mr. Berman, how do you feel about all this?

STATEMENT OF JERRY BERMAN

Mr. BERMAN. Mr. Chairman, I am here on behalf of the Electronic Frontier Foundation, which is an organization concerned with civil liberties in the digital era. I am also here on behalf of the coalition of over 50 communications, computer, and civil liberties organizations that have been opposing the administration's proposals, but also always saying let's work out a more reasonable solution. And I am accompanied by Ron Plesser, from Piper & Marbury, who drafted a report which I would submit for the record which is a long chronology of the efforts by industry to cooperate and to meet the needs of the FBI as they identify problems.

But I want to stress the privacy issues here. The Digital Privacy and Security Working Group really is the outgrowth of the coalition that worked with you and with Mr. Edwards and others in the Congress to pass the Electronics Communications Privacy Act. That was the recognition that we were entering into an era of an information highway, that technologies were converging and that we needed to protect the content of communications being carried over these networks, and also the transactional information that was being generated by these technologies. It was landmark legislation establishing that we had to incorporate these values into the information highway.

Now we have proposals which amount, by the administration and in going through the Congress, to expand the information highway so that eventually voice, data, and video communications by all citizens are going to be carried over this network. We are going to do the real dream of being able to do banking, medical services, political activity, order movies. The whole range of activities that are possible here is coming to fruition, and government is bringing that about by a policy of decentralization and competition and allowing the industry to really make use of its innovation to drive the technology, to get government out of the way.

Here we have on the other side of the fence the FBI and the Justice Department coming in and saying, no, what we really need here is to establish industrial policy and put the Attorney General at the head of the information highway to make sure that we can conduct our wiretapping job. No one disagrees with the need to maintain law enforcement authority, but there is simply no justification on the record for this broad sweeping legislation, which includes broad sweeping new intrusions into privacy.

While the Director said that there was some misleading of the public about the intent in this bill and they have also said that they are prepared to redraft it, that means that something was wrong with this first draft. And what was wrong was that they were saying not only do we want the contents of communications delivered to remote locations through network design, but we want all of the transactional information, the call setup information which is being generated, delivered to remote locations, not simply investigations where there is a warrant but any lawful investigation.

The toll record and the pen register which this may get carved out to is one thing. There are even questions about the broad use and access to that information. But the toll record and billing record of the future is all these transactions we as citizens are going to be doing across this network. It will tell you what movies you are going to be watching. It will tell you what magazines you subscribe to, what doctor you are seeing, where you are at any particular moment.

Congressman Edwards, when I was at the ACLU, we were for years on the NCIC tracking system, the National Crime Information Center, and they might be able to point at people. And we oppose that.

This dwarfs the NCIC. This is NCIC-squared because this really is the real-time transactions, not of people arrested or wanted, but every live American human being dealing in the electronic communications era. So it has to be narrow.

On top of that, to come out with a proposal that says if you do not—this is industrial policy. It says if you do not meet the design here and if a network provider does not meet, we can shut you down. I do not believe that that would stand scrutiny under the first amendment, that failure to meet some requirement for a fourth amendment wiretap could allow the Federal Government to go into court and enjoin Bell Atlantic or AT&T and say you are not operating anymore, the phones are stopped. And that is on the face of this bill.

There are also war powers in here with respect to manufacturers. There is a section in here which says that manufacturers of hardware and software have to meet the requirements that carriers need to meet on a priority basis at reasonable cost. It does not say you get to bid on the software design, but, Microsoft, if you are building the set top box of the future, you design it the way we want it. That is industrial policy. I think it is unconstitutional except in time of war. But it raises enormous questions about the scope of this legislation, and we really have to go back in questions and get to the heart of where the problem is. And I think it can be addressed in much narrower form and without this kind of legislation, and I hold myself open to questions.

My last comment is that I simply applaud the fact that Congress is getting into this. We have been having a dialog. I speak on behalf of this coalition for 2 years with the administration, the Bush administration and Clinton administration. And we are like ships passing in the dark. There is a great deal of separation between the private sector, industry and civil liberties, and the administration, and it needs Congress to bridge that gap if we are going to solve law enforcement problems and continue to keep a balance with our privacy rights in the United States.

Thank you, Mr. Chairman.

[Mr. Berman submitted the following:]

PREPARED STATEMENT OF JERRY BERMAN AND RONALD L. PLESSER

Chairman Leahy, Chairman Edwards, and Members of the Subcommittees: We appreciate the opportunity to testify today on the Clinton Administration's draft legislation, "the Digital Telephony and Communications Privacy improvement Act of 1994." I am the executive director of the Electronic Frontier Foundation (EFF), a public interest organization dedicated to achieving the democratic potential of new communications and computer technology. With me today is Ronald Plesser, a partner at Piper and Marbury and counsel to EFF on digital telephony issues.

I. THE DIGITAL PRIVACY AND SECURITY WORKING GROUP

We appear today on behalf of EFF and on behalf of the Digital Privacy and Security Working Group (DPSWG), a coalition of more than 50 computer, communications, and public interest organizations and associations working on communications privacy issues since 1991 under the coordination of the Electronic Frontier Foundation.

Senator Leahy, we must give credit where credit is due. The DPSWG has evolved as a direct result of your privacy policy initiatives. In 1986, many of the organizations and individuals in the working group joined together to support your successful effort to enact the Electronic Communications Privacy Act of 1986 (ECPA), landmark legislation establishing early on that public policies must and can be devised to ensure that the emerging information superhighway operate in a manner consistent with privacy, free speech, and other core democratic values. In 1991, many of the organizations in the DPSWG participated in the "Ad Hoc Leahy Task Force" which you tasked to look at how ECPA was faring and to make recommendations to you for improving communications privacy protections.

II. BACKGROUND ON DIGITAL TELEPHONY

The Digital Privacy and Security Working Group has had to spend most of its time responding to government initiatives that would change and modify the principles that underlie ECPA. The Clinton Administration's Digital Telephony and Communications Privacy Improvement Act of 1994 is only the latest in a series of government initiatives put forward over the past few years to seek to resolve law enforcement's perceived problems in conducting wiretapping in the era of digital communications.

In each and every case, the members of the DPSWG, from AT&T to the United States Telephone Association, from the ACLU to EFF, have uniformly sought to identify the specific technical concerns of the FBI and law enforcement. This has not been easy and, frankly, we continue to believe that the FBI has not made its case. On a policy level, there is little disagreement that the FBI and law enforcement should continue to be able to conduct wiretaps in a digital environment. On a technical level, their concerns are global and their resolutions are general. The resolution of this issue should be through carefully crafted solutions so as not to upset the balance between law enforcement interest and continued confidence in the public switched network. The proposals that we have seen are over-broad and would create more problems than they would resolve. In short, the FBI has not made a technical case that supports the sweeping changes that it seeks.

- In 1991 the Bush Administration proposed a "Sense of the Congress Resolution" that would have interpreted current wiretapping statutes to require communications carriers, network operators, and service providers to turn over the "plain text" of all communications for law enforcement purposes. The DPSWG argued that the proposal was unworkable and vague, and its efforts led congressional leaders to remove the provision from pending omnibus crime legislation.
- In 1992 the Bush Administration circulated Digital Telephony No. 1, draft legislation that would have required all providers of electronic communications services to obtain an FCC or Attorney General Certification that their networks or facilities meet evolving FBI electronic surveillance requirements. In September 1992, the DPSWG published an "Analysis of the FBI's Digital Telephony Proposal," signed by 35 computer, communications, and civil liberties organizations and associations highly critical of the digital telephony draft legislation on privacy, security, and economic cost grounds. This analysis, a copy of which we submit for the record, convinced Congress to reject the Bush Administration's proposal.
- Last year, the DPSWG, based on optimism about the Clinton Administration's information highway program, began work on a "white paper" designed to set forth new policies to enhance privacy and security in the context of the emerging National Information Infrastructure. When the Clinton Administration announced its "clipper chip" encryption escrow plans and intention to conduct a high level review of privacy, encryption, and related policies in April 1993, the DPSWG turned its attention to addressing the Administration's concerns. On November 24, 1993, we submitted a draft report to the Administration that presented a detailed case against the need for legislation like digital telephony to resolve law enforcement surveillance problems. The FBI stated that it had concerns with the report, but has refused to state the basis for any of its concerns. We submit a copy of our November report for the record.

III. THE DIGITAL TELEPHONY AND COMMUNICATIONS PRIVACY IMPROVEMENTS ACT OF 1994

Despite our concerted efforts, the Clinton Administration has now proposed its own bill, the Digital Telephony and Communications Privacy Improvement Act of 1994. Responding to the February draft bill on March 9, 1994, 20 members of the DPSWG, including AT&T, MCI, USTA, Business Software Alliance, Software Publishers Association, Apple Computer, the American Civil Liberties Union, and the Electronic Frontier Foundation sent a letter to the President and Vice President stating strong opposition to the new version of digital telephony. On March 11, the DPSWG sent its initial analysis of the legislation to FBI Director Louis Freeh, which reiterated that the legislation is unnecessary and, as drafted, could undermine communications privacy and citizen confidence in the public switched telephone network.

The Clinton Administration's proposed digital telephony legislation would:

- Require carriers to provide real-time remote access not only to the contents of communications data sought pursuant to a judicial warrant but also to call setup and other transactional data sought in any lawful investigation;
- Require suppliers of hardware and software to telecommunications providers to meet law enforcement requirements on a priority basis at reasonable cost; and
- Empower the Attorney General to seek to enjoin a carrier from operating who was not in compliance with law enforcement requirements and to impose significant fines on carriers and suppliers who fail to meet law enforcement demands.

1. The legislation threatens privacy rights

As we interpret the draft legislation, it would require a service provider to hand off not only the contents of communications but deliver to remote locations "call setup information" whether or not incident to a warrant issued for wire, oral, or electronic communications as set forth in 18 U.S.C. § 2518. Extending the legislation's scope beyond the acquisition of content (pursuant to a warrant under § 2518) to the independent acquisition of call setup information raises many issues that require examination.

For example, currently the legal standard for obtaining transactional data is a certification (via subpoena or statement to a judge) that the sought-after data is relevant to an ongoing criminal investigation. In the era of personal communications services (PCS) and the information highway, transactional data will reveal far more about individuals than it has in the past. In fact, in some cases it may be equivalent to content information. This transactional data certainly could make it possible to build a detailed model of an individual's behavior and movements. The net result could be government dictating to industry that it create a surveillance-based system that would allow federal, state, and local governments to use a service provider's electronic communication facilities to conduct minute-by-minute surveillance of individuals.

As long as they have an IRS or other administrative subpoena or a law enforcement agent willing to certify that the sought-after data is relevant to an ongoing criminal investigation, law enforcement officials could demand that they be notified at some remote location every time certain individuals communicate by telephone, and their location at the time, as well as every database they connect to and when they log on and off. In short, law enforcement officials could insist on instantaneously knowing the existence of every single electronic communication (but not its content).

The enormous potential for abuse and threat to personal privacy suggests that, if transactional data were to be covered by digital telephony legislation, it should be incidental to a "Title III" wiretap warrant. This would not limit in any way law enforcement's access to trap and trace, pen register, or call billing information under current law or practice. This is particularly true given that no case has been made that demonstrates any current or potential difficulty in getting this noncontent information under current practices. The technology in fact has made these types of services much easier for law enforcement to use and access. Additional legislation is simply not necessary to obtain this data.

2. We do not know what is covered

The obligation to isolate the content of communications must be reasonably related to the service provider's telecommunications services. It would be unreasonable for the FBI to demand any person involved with the communication to furnish it with access to that communication. For example, most providers, including local telephone companies, usually need to isolate communications for purposes of billing and maintenance. It is appropriate for the FBI to seek their assistance in intercepting communications on their networks only when the requests are reasonably related to the telecommunications services they provide.

Therefore, the question is not necessarily who is covered, but what telecommunications services are covered. For example, the legislation should reflect the fact that, in reselling services, even local telephone companies sometimes are unable in those instances to furnish call setup information regardless of whether it is incidental to the acquisition of a communication's content.

3. It is not clear what requirements would be placed upon service providers and what standard of compliance would be applied

Legislation should carefully define the obligations of service providers. This is not the case with the FBI's current draft of proposed legislation. These obligations are vague and subject to considerable interpretation. Service providers and manufactures must have flexibility to adopt procedures that reasonably comply with the specific functional performance requirements of law enforcement.

This is particularly true where, as here, compliance requires an assessment of future needs and interoperability requirements. There is a difference between compliance and a guarantee, and legislation must reflect that difference. Carriers should be required to provide reasonable cooperation and that cooperation should be measured by a standard of reasonable compliance.

In installing new software or equipment under this statute, a service provider must be able to reasonably assess future demands by law enforcement. Other industries subject to regulation at least know, for example, the temperature at which they must maintain the specimens, the emission standard they must satisfy, or the type of safety restraint equipment they must install and the date by which they must have it installed in vehicles. Service providers cannot be held to an absolute standard of compliance where they are using and delivering new technologies to the public and the demands of law enforcement are not clearly specified. This applies to both capability and capacity. Law enforcement must be specific in its requirements for capacity and capability from each service provider.

4. Issues arise as to what is expected of commercial mobile service providers

It is not a foregone conclusion that mobility in a digitized telecommunications environment will degrade or otherwise impede the law enforcement community's ability to effectively execute court-approved wiretap orders.

Wireless carriers are committed to assisting law enforcement agencies to successfully wiretap and intercept voice communications. To accomplish this goal, the wireless industry understands that available excess port capacity is needed in all switches throughout the nation. While it may be reasonable for federal and state law enforcement agencies to acquire the contents of wireless communications pursuant to "Title III" warrants through additional port capacity, it would be prohibitively expensive to require that every one of the nation's switches be connected to the FBI to enable it to acquire such information on a "real time" basis at remote locations.

Connecting every one of the nation's switches to the FBI, moreover, would increase exponentially the risk of unauthorized access to wireless communications. Further, the proliferation of fraudulent use of wireless telephones through such techniques as "cloning" and "tumbling" ESN's (electronic serial numbers) poses additional questions with respect to privacy and the ability of law enforcement to properly execute court-approved wiretap orders.

5. It is uncertain what the responsibilities of manufacturers and suppliers are under the legislation

The FBI wishes manufacturers of telecommunications equipment and providers of support services to fall within the scope of the legislation. But, would service providers be held liable for software or hardware that is not available from vendors? Why? How would the obligations be enforced against foreign manufacturers? What would be the liability of a domestic carrier that relies upon foreign manufacturers? What are the trade implications of having domestic manufacturers export equipment designed for governmental surveillance?

6. Serious issues are raised as to how, and during what period, costs are to be recovered to ensure that there is a direct relationship between the costs reasonably incurred by covered entities and the government's requirements

Government should pay for what it needs, which will help focus attention upon the facilities that truly need upgrading. If the government does not pay for upgrades or facilities, then the service providers should not be held responsible. The FBI appears to have accepted the concept that government should pay for the costs of compliance but has so far underestimated these costs and proposed an arbitrary three-year limit on cost reimbursement. Government compensation should be ongoing with industry's compliance.

IV. IS THIS LEGISLATION NECESSARY?

The most fundamental question that needs to be resolved is whether this legislation is necessary. In our view neither the Bush nor Clinton Administrations have made a persuasive case. They argue that electronic surveillance is essential to law enforcement, but they have not demonstrated that their access to communications subject to judicial warrants have been impaired. They have pointed to problems encountered with call forwarding and cellular communications, but carriers have been able to meet new requirements through cooperative efforts. In the report prepared for the Clinton Administration and sent to the FBI last November, the DPSWG presented the following case:

- First, there is no evidence that current law enforcement efforts are being jeopardized by new technologies. As described in our attached report, a Freedom of Information Act request made by Computer Professionals for Social Responsibility turned up evidence that not one law enforcement agency could demonstrate that digital telephony has interfered with any electronic surveillance activities.
- Second, industry is cooperating with appropriate authorities to avoid future problems and to expand existing capacities.
- Finally, given this lack of ascertainable concern now or in the future, it is not justifiable to require all providers, including telephone companies, packet switching networks, computer and software manufacturers, and the like, to be subject to new design standards and requirements. This is particularly the case where such requirements may in some cases severely limit the development of the new national infrastructure and once again lessen the American public's confidence in our communications networks.

ECPA was enacted to reaffirm the confidence of all Americans that their communications whether aural or digital, common or private, voice, date, or video are secure from unauthorized interceptions. The government has the current authority and ability to adequately intercept electronic communications when authorized to do so. Sufficient reasons to amend this statute now to allow the government to dictate the design of communications technology just do not exist.

V. CONCLUSION

We applaud the fact that Congress is holding these hearings. Only Congress can resolve whether or not legislation is necessary and work to bridge the considerable division between the Administration and the private sector. We welcome the opportunity to state our views, and are ready and anxious to work with you and the Administration to find solutions to law enforcement needs that strike a balance between those needs, privacy, and other significant societal interests.

Interim Report of the Digital Privacy and Security Working Group on the FBI's Digital Telephony Proposals

INTRODUCTION AND SUMMARY

The Electronic Communications Privacy Act of 1986, ("ECPA," P.L. 99–508), established the current legal framework for the interception of electronic communications. Prior to ECPA the only relevant statutory provisions were set forth in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("the Wiretap Act," P.L. 90–351). The Wiretap Act covered only common carrier communications that were aurally intercepted. With the range of new communications technologies coming on-line in the 1970's and 1980's, the law had obviously become obsolete. ECPA was designed to provide the public with a sense of privacy and security in the new range of data communication services, many of which were provided by noncommon carriers and hence were "unprotected" from a legal standpoint.

ECPA amended the Wiretap Act by establishing procedures through which the government can obtain access to electronic communications held or transmitted by electronic communications service providers. It covers traditional voice communications as well as data communications. Data communications includes electronic mail and other computer-type communications that often are stored in the process of dissemination. In the years since its enactment, ECPA has worked well.

An essential part of ECPA is the technical ability to effect access or interception. ECPA requires that electronic communications service providers furnish the government with technical assistance in completing authorized interceptions, as it should. Local telephone companies, long distance providers, electronic mail providers, cellular services and other providers all have solid records of compliance with authorized requests for interception.

Law enforcement, however, has asserted that the continued advent of digital communications and the modernization of the national information infrastructure (NII) requires an amendment to ECPA in order to ensure a broader level of assistance by electronic communication service providers. We do not agree.

The government should not have the ability to dictate how communications services are provided or how they are designed. *First,* there is no evidence that current law enforcement efforts are being jeopardized by new technologies. *Second,* industry is cooperating with appropriate authorities to avoid future problems and to expand existing capacities. *Finally,* given this lack of ascertainable concern now or in the future, it is not justifiable to require all providers, including telephone companies, packet switching networks, computer, software manufacturers, and the like, to be subject to new design standards and requirements. This is particularly the case where such requirements may in some cases severely limit the development of the new NII, hamper American competitiveness in the technology, and once again lessen the American public's confidence in communications products.

ECPA was enacted to assure Americans that their communications whether aural or digital, common or private, are secure from unauthorized interceptions. The government currently has both the authority and the ability to adequately intercept electronic communications when authorized to do so. Sufficient reasons to amend this statute now, to allow the government to dictate the design of communications technology, just do not exist.

A. BACKGROUND

In recent years the U.S. Government has been advocating a legislative solution to the law enforcement challenges posed by new communication technologies. In 1992, for example, the Federal Bureau of Investigation (FBI) unveiled a digital telephony legislative proposal (known internally as "Project Root Canal"), which would have imposed mandatory system design requirements. The draft legislation would essentially force industry to perpetually accommodate current surveillance equipment and procedures, and would thus significantly retard the development and deployment of new telecommunications technologies. While the proposal received attention from the press, the General Accounting Office (GAO), and others; no such legislation was introduced in Congress.

The National Institute of Standards and Technology (NIST) has requested the Digital Privacy and Security Working Group's (DPSWG) recommendation on how the government should cope with the new technologies. NIST has specifically asked whether DPSWG can develop a means of ensuring access to digitized communications that preserves, but does not extend, the government's current authorities.

DPSWG acknowledges that law enforcement officials need adequate communications interception tools to do their job. We believe that continued cooperation by government and industry within the working relationship that has emerged from the 1992 Quantico Joint Government Industry Group will resolve "the digital telephony problem" and preserve the government's current authorities. The discussions have succeeded in identifying specific problems and have begun the process of generating concrete, cost-effective solutions. This process has facilitated a more robust exchange of technical information and an identification of possible new equipment and police tactics needed to achieve law enforcement goals. We do not believe that new legislation is needed or advisable.

Before proceeding, we set forth our understanding of "the digital telephony problem," the FBI's proposed solution, and the U.S. Government's current authority both to intercept communications and to compel assistance by providers of electronic communications in such interceptions. We also underscore the importance of distinguishing between legitimate areas of mutual concern and rhetorical characterizations of the digital telephony problem.

1. What is the "digital telephony problem"?

According to the FBI's Digital Telephony proposal, "advances in technology, and undoubtedly the future introduction of new technologies, will soon make it impossible for law enforcement agencies to effect lawful court orders to intercept electronic communications."[1] Pointing to advanced cellular technology and new digital features that "have already frustrated orders," the FBI notes that "[t]his happened because the legitimate needs of law enforcement were not considered during the design and development phases of the systems."[2]

The solution, according to the FBI, is legislation mandating the telecommunications industry to accommodate the legitimate needs of law enforcement during the design and development phases of new technologies so that, when served with a court order, they will be able "to identify and provide the entire content of specific telephone conversations to the exclusion of all others, regardless of the technology involved."[3]

Specifically, the FBI proposal would impose obligations to provide various generic interception "capabilities and capacities" and empower the Attorney General to grant exemptions, after consultation with the Federal Communications Commission, the Department of Commerce, and the Small Business Administration. Any person who manufactured equipment or provided a service that did not comply with the broad and vague requirements of the proposed statute would be subject to a civil penalty of $10,000 per day. In short, the FBI proposal would grant the government a right to mandate the use of particular technologies, block other technologies, and effectively redesign the communications network and the equipment used by large segments of our society.

Ironically, the FBI concedes that the desired industry-developed "technical solutions" to the needs of law enforcement should, of course, also be both "cost effective" and sensitive to "the intense competitive demands of the market place."[4] Yet, the proposal imposes a burden on the more than 140 million lines or ports existing in the U.S. telecommunications network, rather than the less than 10,000 lines targeted for court-ordered interception, each year, i.e., the five thousandths of one percent (.005 percent) of the network subject to wiretaps.[5]

2. What are the government's "current authorities"?

The Wiretap Act, as amended by ECPA, governs the government's communications surveillance activities. Electronic or wire surveillance requires prior authorization by court order (or, in emergency cases, must be approved by the court within 48 hours of inception). Only upon a showing that satisfies the statutory requirements, may a federal court issue an order authorizing a specified law enforcement agency to intercept a certain type of communication by an identified individual for a definite period of time in order to obtain evidence concerning specified offenses.[6]

Since 1970, federal law has also authorized federal courts, upon the request of a law enforcement agency, to direct telecommunications providers and other persons to furnish "all information, facilities, and technical assistance necessary" to accomplish a surveillance permitted by law.[7] While the statute does not define "technical assistance," the Senate Committee Report accompanying ECPA stated that the provision "is a codification of the cooperative working relationship that exists between telephone companies and law enforcement officials."[8] Further, the report makes clear that Congress did not intend to make the assistance obligation unlimited by, for example, making the telephone industry, "in effect, a branch of Government law enforcement."[9] It certainly reveals no mandate to change the communications networks in order to make authorized interceptions possible.

---

[1] FBI, *Digital Telephony: A Legislative Proposal,* at p. 1 of "Summary of Issues" (Feb. 1993). Although the FBI has recently circulated a new draft of its proposed legislation, the Agency's justifications for the legislation remain essentially the same as in 1992 and 1993.

[2] *Id.* As noted *infra* at part B.5, FBI records about "Project Root Canal" recently released pursuant to a Freedom of Information Act request show that FBI field offices nationwide were reporting that they and other federal, state, and local law enforcement agencies were experiencing "no problems" and "no difficulties" with new telephone technologies at the same time as the FBI was contending that such technologies had "already frustrated" wiretap orders.

[3] *Id.* at p. 2*.

[4] *Id.*

[5] The total number of court-authorized content wiretaps in 1991 was 856 (almost 60 percent of which were at the state level), while the call-set-up or pen register tap orders for 1991 at the federal level were only 2,445, which implies a national total under 7,000. *See* Administrative Office of the United States Courts, Reports on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications (1983–1992).

By comparison, according to the United States Telephone Association, the number of access lines exceeds 140 million.

[6] *See* 18 U.S.C. §2510 et seq. In certain limited circumstances specified by the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §§1802 et seq.), electronic or wire surveillance to acquire foreign intelligence information may not require court authorization.

[7] *See* 18 U.S.C. §§2518(4), 3124; *see also* 50 U.S.C. §1802(a)(4).

[8] S. Rep. No. 541, 99th Cong., 2nd Sess. 29 (1986).

[9] *Id.*

There are no reported court decisions on the assistance requirement since the enactment of ECPA.[10] A review of pre-1986 judicial opinions shows that there have been few instances where telecommunications providers have challenged the propriety of court-ordered technical assistance. In the rare cases that have arisen, the courts have ruled in favor of the government and against the telecommunications carrier.[11]

3. Exaggerations: An illustration

In promoting its digital telephony proposal, the FBI has advanced exaggerated claims that a crisis exists in law enforcement. It is important to keep the claims in perspective when determining what precisely is the digital telephony "problem."

For instance, one example routinely used in the past is the effect of fibre optic cables, which transmit communications digitally, on the FBI's ability to intercept communications. It has been said that FBI agents tapping into fibre optic trunk lines would hear only computer code or nothing at all. Alternatively, tapping a high-capacity fibre optic line would result in the interception of thousands of conversations, making it nearly impossible for FBI agents to find the conversation of suspected criminals in the complex "bit stream." By contrast, with lower speed, lower capacity telephone lines carrying analog transmissions (the electronic signals used by the first telephones in which sounds correspond proportionally to voltage) law enforcement agents can clearly hear conversations.[12]

This characterization of the fibre optic "problem" illustrates two issues. First, it reveals an ignorance of fundamental aspects of the way law enforcement conducts wiretaps today. Second, it shows the unreasonableness of law enforcement's demands if taken to their logical conclusion.

This characterization of the fibre optic "problem" overlooks the fact that wiretaps are made at the local loop, not off trunk lines, regardless of technology. Local loops are the telephone lines connecting homes and offices to switches at telephone company central offices. A telephone company usually has various central offices in a city. The trunk lines connect central offices within a city or between cities. Court-ordered wiretaps operate off the local loop connecting the telephone to be intercepted and the switch of the nearest telephone company central office, not the trunk line.

Because access at one point is all that is needed for wiretapping in any given circumstance, it would be unreasonable for the FBI to demand access to a communication at any point in its transmission on any telephone line, including a fibre optic line. Thus, the fact that fibre optic lines are being deployed is essentially irrelevant. The important issue for law enforcement is the continued ability to isolate individual communications at the customer side of the last switch. As is discussed below, at part B.1.a, industry has teen working with law enforcement to address this issue in the context of recent developments in the decade-long deployment of fibre optic in the local loop, known as digital loop carrier, and more recent deployment of integrated services digital network (ISDN) lines.

The need for isolating individual communications, however, leads to the second issue illustrated by this characterization of the fibre optic "problem": the unreasonableness of law enforcement's demands if taken to their logical conclusion.

Just like it would be unreasonable for the FBI to demand access to a communication at any point in its transmission on any telephone line, it would be unreasonable for the FBI to demand any person involved with the communication to furnish it with access to the communication. Local telephone companies, for example, need to isolate communications for purposes of billing and maintenance. It is reasonable for the FBI to seek their assistance in intercepting communications on their network; the request is reasonably related to the business services provided by the telephone company.

A packet switching company, on the other hand, does not have a need for isolating individual communications. It provides "wholesale," bulk access to trunk lines, bills for its services accordingly, and has no means of finding a specific conversation in the complex "bit stream." Because the company is not set up from a business perspective to isolate conversations, it would be unreasonable for the FBI to seek their assistance in intercepting communications on their network. Indeed, to facilitate responding to such FBI requests, the entire packet switching industry would need to undertake a costly reconfiguration of its services for entirely noncommercial reasons.

---

[10] The last published decision on the technical assistance requirement appears to be *United States* v. *Mountain Bell*, 616 F.2d 1122 (9th Cir. 1980), which held that even in the absence of a federal statute governing governmental use of trap and trace devices for electronic surveillance, federal courts possess the requisite authority to direct a telephone company to assist the government in its use of a trap and trace device.

[11] *See, e.g., United States* v. *New York Telephone*, 434 U.S. 159 (1977).

[12] *See, e.g.,* Anthony Ramirez, "As Technology Makes Wiretaps More Difficult, F.B.I. Seeks Help," *New York Times*, March 8, 1992, at A22.

This would be unreasonable and unnecessary. Such a demand of a packet switching company is akin to demanding that an airline land a jumbo 747, rummage through the cargo compartment, unload the bags of mail, and locate the envelope for which a warrant has been issued, when the envelope can be seized by postal authorities at the sender's or recipient's locality before or after it is shipped by air. Yet, the legislation proposed by the FBI in 1992 was clearly designed to cover any system facilitating two-way conversation, and would have required packet switching companies to modify their business to accommodate "the legitimate needs of law enforcement."

Thus, it is critical to keep the FBI's claims in perspective when determining what precisely is the digital telephony "problem."

B. CONTINUED COOPERATION WITHIN THE WORKING RELATIONSHIP THAT HAS EMERGED FROM THE QUANTICO JOINT GOVERNMENT INDUSTRY GROUP WILL RESOLVE THE DIGITAL TELEPHONY PROBLEM AND PRESERVE THE GOVERNMENT'S CURRENT AUTHORITIES

1. The FBI and the electronic communications industry are engaged in a cooperative working relationship aimed at addressing law enforcement's legitimate needs

The FBI and the electronic communications industry are engaged in a cooperative working relationship aimed at addressing the legitimate needs of law enforcement to lawfully intercept electronic or wire communications and at ensuring that these needs are taken into account during the design and development phases of new technologies. The goal is for electronic communications providers, when served with a court order, to be able to identify and provide the entire content of specific telephone communications to the exclusion of all others, regardless of the technology involved, while ensuring that this goal is accomplished through technical solutions that are both cost effective and sensitive to the intense competitive demands of the market place.

a) The ECSPC

Industry and law enforcement officials have established a permanent forum and a process by which to identify and resolve problems. This forum is the Electronic Communications Service Provider Committee (ECSPC), sponsored by the Alliance for Telecommunications Industry Solutions (ATIS), formerly the Exchange Carriers Standards Association. ATIS is a recognized industry association that seeks to resolve issues involving telecommunications standards and operational guidelines. More than 300 companies participate in ATIS-sponsored committees.[13]

ECSPC, established in March 1993, is the successor to the "Technical Committee," a temporary committee of experts from industry and government, which was established in May 1992 by the Quantico Joint Government Industry Group. The "Technical Committee's" charter was to:

- Develop a process for incorporation of law enforcement's needs into future industry technology standards, technical requirements, and specifications;
- Develop technological capabilities and procedures to permit continued interception by law enforcement of communications that use transition technologies; and
- Monitor and track the timeliness of industry's response to law enforcement's requests for intercepts. The goal is "zero-held intercepts."

Like the "Technical Committee," ECSPC consists of representatives from both industry and government. Its mission is to "establish[] an open, yet secure forum between the telecommunications industry and law enforcement representatives to identify those technical and associated operational issues related to lawfully-authorized electronic surveillance and to develop resolutions to such issues for voluntary implementation by the industry." Representatives from various telecommunication companies and associations regularly attend ECSPC meetings, including:

- Ameritech
- AT&T
- Bell Atlantic
- Bellcore

---

[13] ATIS's Toll Fraud Prevention Committee ("TFPC") was viewed as a possible model for ECSPC because TFPC deals with sensitive issues that require participants to sign nondisclosure agreements.

- BellSouth
- Cellular Telecommunications Industry Association
- GTE
- McCaw Cellular
- MCI
- Northern Telecom
- NYNEX
- Pacific Telesis
- Southwestern Bell
- Telecommunications Security Association
- U.S. Sprint
- U.S. West
- U.S. Telephone Association

Representatives from the following state and federal government agencies regularly attend ECSPC meetings:

- Bureau of Alcohol, Tobacco, and Firearms
- Drug Enforcement Administration
- Federal Bureau of Investigations
- Hudson County Prosecutor's Office
- New Jersey State Police
- New York Police Department
- U.S. Secret Service

ECSPC has been meeting in six- to eight-week intervals. In addition to resolving organizational matters (e.g., by-laws), ECSPC has been addressing problems that law enforcement has identified, in the order of priority that law enforcement has assigned them.

Little or no evidence has been presented to the ECSPC of held orders that require technical solutions. Efforts are under way to better track any held orders that may exist. (Held orders are requests for lawfully-authorized electronic surveillance that electronic communications service providers are unable to fulfill at the time they are made.)

Law enforcement representatives report to their industry counterparts on the ECSPC that they are satisfied with this forum, and the dedication and seriousness of the participants. A recent published report that FBI officials were still dissatisfied with industry[14] has stimulated the ECSPC to accelerate its pace even further.

b) ECSPC Action Teams

Four separate "action teams," staffed by representatives of both industry and government, meet more frequently than does the full ECSPC to check transition technologies against law enforcement's "nine requirements." These teams propose technical solutions which are then checked with operational staff and the Telecommunications Security Association. Where appropriate, vendor requirements are drafted.

The areas that have been the focus of ECSPC's work include:

- Digital loop carrier
- Custom calling features
- Integrated services digital networks (ISDN), and
- Cellular communications

Each of these will be discussed in turn.

I. DIGITAL LOON CARRIER

Deployment of digital fibre optic cable in the local loop began over ten years ago. It presented no problem for law enforcement as long as communication providers were able to isolate individual communications at the customer side of the last switch. Design improvements have enabled the fibre to be integrated directly at the switch. This requires communication providers and law enforcement officials to devise new methods (e.g., test ports) of isolating individual communications at the customer side of the last switch, which may now be fully integrated at the switch.

---

[14] See Paula Bernier, "FBI Says New Technology Hinders Wiretaps, Seeks Re-engineering," *Telephony*, Aug. 16, 1993, at 7 & 14 (quoting Barry Smith, supervisory special agent of congressional affairs for the FBI, as complaining that "no solutions have been forthcoming" by the ECSPC to cellular and call forwarding problems).

II. CUSTOM CALLING FEATURES

Switch-based custom calling features such as call forwarding, which allows a user to transfer calls to other phones, challenge law enforcement's ability to follow calls. Because wiretaps are installed at the customer side of the last switch, a law enforcement agency may be lead to believe that no calls are being made when in reality all the calls are being re-routed at the switch. When call forwarding features could only be accessed through customer purchased equipment placed on the customer's premises, law enforcement could follow the calls because the calls went through the local loop and were redirected at the customer's premises. With switch-based features, the calls are redirected at the switch and do not pass through the local loop at all.

III. INTEGRATED SERVICES DIGITAL NETWORKS (ISDN)

Integrated Services Digital Network (ISDN) is an increasingly popular technology that converts today's analog telephone lines into digital signals. Digitization offers much higher data capacity, better audio quality, and greater control over advanced telephone features.

Just like a regular telephone jack will not work with an ISDN line, law enforcement cannot use the same equipment to wiretap an ISDN line that it uses to tap a traditional analog voice telephone line. A basic ISDN line has six channels—two in one direction, two in the other, and two "signalling" channels (one in each direction), which the system uses continuously. Tapping these lines requires the ability to sort out the two channels being used by the suspected criminal from the remainder of the bit stream.

As is the case with other new technologies mentioned here, telephone company engineers have already identified readily available technology that can be used to enable law enforcement to maintain their surveillance capabilities on new, ISDN lines. Nearly two years ago, Bellcore technicians demonstrated to law enforcement officers that commercially-available ISDN testing equipment can also be used to tap into ISDN lines. Even though one ISDN line actually carries up to six data streams, the standard equipment used by Bellcore enables law enforcement to separate out each individual data stream for surveillance.

The days when law enforcement officers climb up telephone poles and tap into a conversation by attaching alligator clips directly to the telephone line are dwindling in number; in the majority of jurisdictions law enforcement officers prefer to have the tapped communications rerouted to a remote, safer location. ISDN may precipitate the end of these remaining "field taps." To the extent that a field tap is still required, however, these days the officer is well advised to bring along a hand-help device called an ISDN protocol analyzer. Such devices are readily available for about $2000.

IV. CELLULAR COMMUNICATIONS

Cellular telephony can present both capacity and technical challenges to law enforcement.[15]

Let's first compare interception of noncellular communications to interception of cellular communications. Keeping in mind that access at one point is all that is needed for wiretapping, the wiretap target's location is always known in noncellular telephony. The nearest central office can be identified, and the telephone company can furnish the police with the target's cable make-up for interception. By contrast, because cellular's mobility allows its users to send and receive calls from multiple points, the target's location can change throughout the day, or from day to day. As the target moves, his or her calls originate at or are handed off to a different cell site. This has forced cellular service providers to establish wiretap connections at a central location on the provider's premises.

The capacity problem arises when a cellular service provider exhausts the ports at which wiretap connections can be made. In the New York City area, a cellular provider for several years had the capacity for handling only twelve such simultaneous wiretaps. Until this situation was corrected, the capacity limitation determined the provider's ability to service requests for court ordered wiretaps.

---

[15] It is important to distinguish those issues arising out of limitations in communications equipment *capacity* from those arising out of communications equipment *design* characteristics. The former may be peculiar to a particular service area or region due to an unusual demand for wiretaps, the nature of a particular service provider's network equipment, or the geography. The solution to any problem may lie in the acquisition of certain equipment by the particular service provider or by the particular law 'enforcement operation. The latter issue, by comparison, reflects a technical matter inherent in the technology as it is deployed anywhere in the country.

The process of developing appropriate equipment to resolve this capacity problem also illustrates the substantial efforts that industry expends to respond to law enforcement needs. In 1991 a telecommunications equipment manufacturer unveiled a cellular surveillance system that would resolve the New York City capacity problem. The system had required two years to develop. The system permitted real time remote surveillance through the public switched network, which would have enabled law enforcement officials to conduct an unlimited amount of simultaneous wiretaps. In addition, it offered many advantages over the existing surveillance technology, including coast-to-coast remote monitoring capability on short notice.

While law enforcement officials wished to overcome the capacity problem, they also needed to have the "call set up information" (which identifies the calling and called parties) forwarded to them in the same medium as the content of the communication. The rationale for this requirement is authentication concerns that arise with evidence in criminal prosecutions. Unfortunately, while the new system made the call set up information available concurrently with the communication content, it was available only in a separate medium. In resolving one problem, the manufacturer had created another one. Because of law enforcement's unwillingness to present new authentication issues to the courts, two years of research and development had been wasted and resolution of a law enforcement problem had been further delayed. It was not until the summer of 1993, after modifying the equipment in 1991 and undertaking a series of field tests of the modified equipment in 1992, that the manufacturer was able to begin deploying the new equipment.

A different problem is presented by cellular roaming arrangements. Through roaming, a target can send and receive calls outside of the cellular company's service area. The wiretap connection at the cellular service provider's premises does not intercept the target's calls. Thus, a New York City target who uses his cellular telephone in New Jersey to call Philadelphia frustrates the court-ordered wiretap connection installed on the premises of his New York City cellular service provider: the call originates in the New Jersey cellular provider's service area and terminates in the Philadelphia cellular provider's service area. This problem reflects a technical issue arising out of the inherently mobile design characteristics of cellular communications equipment.

* * * * *

ECSPC action teams are developing reasonable, affordable, and effective means to be used for authorized interceptions in these circumstances. In some cases, new surveillance techniques, equipment, and skills may be necessary, too.

So far this process has generated at least five final or draft "contributions," which report on a problem and propose possible solutions. The contents of these reports are confidential and subject to the terms of the nondisclosure agreement under which ECSPC and its participants operate.

The ECSPC has even begun to apply the same approach to *new* technologies by establishing an action team to address the new family of wireless services known as personal communications services or "PCS," which the FCC has yet to license. Examining technologies before they are widely deployed will help industry and law enforcement to "stay ahead of the curve" rather than having to "play catch-up."

2. The forum and process that industry and law enforcement have jointly established will satisfy the government's need to maintain its ability to lawfully intercept communications

ECSPC provides a much-needed forum and process for the telecommunications industry and government to communicate with each other about technical developments and needs.

According to the FBI, advances in technology threaten to make it impossible for law enforcement agencies to effect lawful court orders to intercept electronic and wire communications, and this obstacle can only be avoided by having industry design new technologies according to government specifications.

While the FBI sought, as part of its legislative proposal, to have Congress mandate that industry accommodate these law enforcement needs,[16] the reality is that the FBI and the electronic communications industry are now engaged in a cooperative working relationship aimed at addressing these needs and at ensuring that they are taken into account by industry as they develop new technologies. This process has facilitated a more robust exchange of technical information and an identification of possible new equipment and police tactics needed to achieve law enforcement goals.

---

[16] *See* FBI, *Digital Telephony: A Legislative Proposal,* at pp. 1–2* of "Summary of Legislative Proposal" (Feb. 1993).

This process would have been necessary even if legislation had been enacted. The process facilitates the functional responsiveness of electronic communication providers and their equipment manufacturers to law enforcement's needs. This functional responsiveness is accomplished through technical solutions that are both cost effective and sensitive to the intense competitive demands of the market place.

The ECSPC also is capable of evolving and adapting as needed to address future challenges identified by industry or government.

3. The forum and process that industry and law enforcement have jointly established respond to GAO's criticism of the FBI

Furthermore, the forum and process that industry and law enforcement have jointly established respond to GAO's criticism that the FBI had failed to (1) communicate with industry, (2) define its wiretapping needs, and (3) permit industry to analyze these needs.[17]

The FBI defined its wiretapping needs in a 20-page document entitled "Law Enforcement Requirements," which it circulated in July 1992. The requirements are designed to permit law enforcement officials to conduct real time monitoring and recording at their facilities of both the content of the communication and information identifying the calling or called party, in the same signal form as the communication is transmitted, whether the target is stationary or mobile, and without detection or degradation of service.

The FBI's role in establishing and participating in the ECSPC facilitates communication between industry and law enforcement, and permits industry to analyze law enforcement's wiretapping needs in light of current technologies and during the design and development phases of new technologies. The discussions have succeeded in identifying specific problems and have begun the process of generating concrete, cost-effective solutions.

The delays experienced in developing a cellular surveillance system to solve the New York City capacity problem, discussed above at part B.1, illustrate the importance of this process of dialog and analysis. The ECSPC will help prevent the type of waste and delay that occurred there.

By comparison, had the FBI proposal been law in the 1980's, it would have blocked the deployment in the U.S. of wireless technologies, such as cellular telephony, damaging our national economy and the balance of trade.

4. The ECSPC preserves but does not extend the government's current authorities

The working relationship that has emerged from ECSPC permits electronic communications providers and their equipment manufacturers to reasonably anticipate problems that could arise in a company's furnishing of the technical assistance necessary to accomplish lawful electronic surveillance. By developing with law enforcement technical solutions to obstacles posed by technologies, service providers—when served with a court order—are able to identify and provide the entire content of specific telephone communications to the exclusion of all others, regardless of the technology involved. The discussions also alert the law enforcement community to the occasional need to make changes in police surveillance tactics.

5. No legislative solution is required because no technological or law enforcement crisis exists

Virtually no evidence has been presented of held orders that require technical solutions. Indeed, FBI records about "Project Root Canal" recently released pursuant to a Freedom of Information Act request show that FBI field offices nationwide were reporting that they and other federal, state, and local law enforcement agencies were experiencing "no problems" and "no difficulties" with new telephone technologies at the same time as the FBI was telling the Congress and the press that such technologies had "already frustrated" wiretap orders.

This paucity of evidence of difficulties confirms that no crisis exists that cannot be addressed through this new forum and process. No legislative solution is needed. There certainly is no need to grant the government the right to mandate the use of particular technologies, block other technologies, and effectively redesign the communications network and the equipment used by large segments of our society. If law enforcement is dissatisfied with either the forum or the process, it would be appropriate to consider alternatives. * * *

---

[17] *See* General Accounting Office, *FBI: Advanced Communications Technologies Pose Wiretapping Challenges*, at 4 (July 1992) (GAO/IMTEC–92–68BR).

Senator LEAHY. I yield to Senator Specter to go first with questions, and then Chairman Edwards, and then I will ask some questions.

Senator SPECTER. Thank you very much, Mr. Chairman.

Mr. Neel, I was very interested in your testimony about the cost factor, and I understand that if there is to be value for the Government on law enforcement, the Government ought to pay for it. I agree with that completely. I think it is possible to appropriate the moneys and have the adequate guarantees that the costs will be paid. Furthermore, on the determination of reasonable cost we could perhaps structure an arbitration system and set some time limits so that there is adequate consideration for those realistic matters.

If that were structured, would you withdraw at least that facet of your objection?

Mr. NEEL. Well, it would be an improvement. I think, as always, the critical thing there is reasonable cost and, you know, expeditious payment. Very honestly, the Government might have a different definition for a reasonable amount of time to pay, and you could get into quite a long harangue about the reasonableness of a particular cost. Already this industry has faced that in a couple of cases where compensation was in order, and they just simply wrote the bills off.

Senator SPECTER. Well, we could specify time. We could make it 60 days or 30 days or 90 days, and as to a reasonable cost, we could structure a procedure to determine that.

Let me move on to some of the other points that you made.

Mr. NEEL. Clearly that would be an improvement, Senator, but it is important to make sure that that money is available in the out-years as well, because this will be a permanent problem as new technologies are developed.

Senator SPECTER. Well, I think that is a fair request on your part, and I think we can meet that. When you talk about other networks and that criminals are not stupid, I quite agree with you that they are not stupid at all. But sometimes they are careless, and that is evidenced by the arrest made in Philadelphia yesterday, and I commend the telephone companies for their cooperation. When you noted that facet, you are exactly right. And I think we have to work on the structure of the exceptions, and I believe that we need the assistance, the FBI needs the assistance of the telephone companies to give them information as to how you structure the exceptions so that there is realistic law enforcement at work. But I think that has to be attempted.

You talk about competition. Maybe some of your competition will be discouraged from competing with all these onerous requirements if we pass a law like this. You may have——

Mr. NEEL. Well, unfortunately, in this legislation, many of the competitors of local telephone exchanges would be exempted under this. So while this is certainly not a reason not to redouble anticrime efforts, it is clearly inequitable for the local telephone exchange to bear this entire burden.

Senator SPECTER. Well, I think we have to work on the exceptions so that it is fair all the way around. I sense from your testimony, in toto, that the telephone companies are prepared to cooperate, as you always have, if it is fair and if you do not have to pay the costs of it if it is done by the Government and the payment is by the Government and that it is fair all the way around. So we will work with you on that. We want to address those concerns.

Mr. PLESSER. Senator, can I have permission to add one response to that?

Senator SPECTER. Go ahead.

STATEMENT OF RONALD L. PLESSER

Mr. PLESSER. The issue is cost, but it is not only cost. The question is: What are the standards applied in the legislation? There was a lot of discussion this morning about this legislation putting requirements. If you read the legislation, there really are not any specific requirements. It is really very, very generalized, and really the question is not just the cost of doing it, but what are the requirements. And that is both a cost issue and a privacy issue for the general public because the way the structure of this bill is, the Attorney General can seek an injunction enjoining the provision of service of any common carrier. So, indeed, call forwarding could be sought to be enjoined if it did not get to a vague standard.

There is no process in here—it is not just an arbitration on the price. There is no process in the provision to establish what those standards are and what the expectations of the telephone companies are to respond to them.

Senator SPECTER. Well, it is very difficult to articulate those standards, and that is something we have to work on. And it is going to require technical assistance from the telephone companies, and I want to talk to Mr. Berman in a few minutes about the privacy issue. But it seems to me that we can work it out. We have to know a lot more than we know, and this subcommittee is going to have the responsibility for markup. But we are going to need your inputs, and there may be some areas in which we are going to have to do the best we can, see how the problems develop and be available to you.

But the severity of the need is extreme. The complications on the technology are overwhelming. We do not know what is going to happen. We just have to do the best we can.

When Mr. Neel talks about the fact that there may be some other developments, or perhaps the chairman raised that, we just have to see what develops along that line and do the very best we can. But we need your inputs on it.

Let me turn to you, Mr. Berman, because I do not want to take too long, and I have deferred my other commitments for a moment. The issue of civil liberties is something about which we are all very, very concerned, and we want to see that met. When I was district attorney of Philadelphia a long time ago, I opposed wiretapping because I thought we could get along without it. And given what has occurred on the crime problem, we are past my individual judgment on that. Pennsylvania did not have wiretapping when I was district attorney, and now it is a matter of working it out as best as we can.

I think you put your finger on a critical aspect when you talk about the responsibility of the phone company beyond situations where there are warrants. My question to you: If this was limited to only the establishment of probable cause before the neutral magistrate, the Federal judge, would that satisfy a large area of your concern?

Mr. BERMAN. I think it would, sir, but there are still issues raised by call setup information which, if it is the judgment that Congress go to legislation—and I am not convinced that legislation is necessary here because the record of cooperation has been good when the FBI has been able to specify what its requirements are. But if we get into the issue of legislation, I think that the creation of these new streams of transactional information, the very detail of it which makes it in many respects more worthwhile to law enforcement, to marketers and so forth than the contents of communications themselves, we may have to—the civil liberties position would be let's revisit the standards under which we access that kind of information so that it is a probable cause warrant, it is incident to a probable cause warrant, but in lawful investigations what should the standard be for any kinds of transactional information? Should it be simply merely it is relevant to a law enforcement investigation?

We now have a reasonable suspicion standard for video records because of the Bork incident. In other words, there are higher standards for that kind of record under statute now, but this kind of information, this kind of sensitive information, is not simply limited to video records. It is whole categories of records and information that is going to be out on the information highway. So why don't we consider in the context of legislation, if we are going to get into legislation, a new warrant requirement for transactional information?

Senator SPECTER. I am prepared to do that. When you say you doubt that legislation is necessary, my sense is that legislation is necessary, if only to deal with the problems of cost. This is a governmental expense, and we are going to have to pay for it. You talk about the various standards. We are prepared to work with you on identifying what those various standards are.

We have had some experience in structuring those standards, and we are prepared to listen to your areas of concern. You talk about telling what movies and magazines people see and read and who their doctors are, I do not want to see that kind of information available, and I am sure that the FBI does not either. It is a question of how we structure this. If we can figure out all the technology and the wonders that we are working on now, we ought to be able to figure out the technology to limit it. But that will have to come from the experts.

Mr. BERMAN. We are going to have to relate to a couple of other privacy issues that I have not stressed and I would like to just mention.

One of the problems with network design, for the last 10 years, as we have built toward this information highway—and I use the royal "we"—government, because of computer crime and other security concerns, industrial espionage, the fact that we are moving banking transactions and information across this information highway, has been urging industry, rightly so, to build more secure networks. So they have been building more secure networks. And, in fact, it is because more security is really the answer to lots of computer crime in this new digital era.

On top of that, here comes the administration and it says because of other crime issues, which they would like to look at separately, they are talking about creating holes in the network or potential holes to be able to do wiretapping which others might be able to exploit from computer crime to gain access to financial information and so forth.

So it is a very complicated issue of about where the security balance is here and the privacy issues are here.

We also have a government which is saying that our communications are moving into a wireless era, and Senator Leahy is holding hearings after the recess on this issue. What was recommended by industry to protect the privacy of communications, these new sensitive communications, is encryption, that we need to scramble these communications in order to protect it against private intrusion. The cellular, the Robb-versus-Wilder, can be duplicated on the street all the time. And we are moving into PCS where everyone is going to carry their phone around, and it is out in the open.

You need technical solutions to that. An industry-civil liberties task force recommended to Senator Leahy in 1991 that we move toward those solutions, but the Government has decided that they are going to impose their own security device, which is very controversial, the clipper chip encryption device developed by NSA. And they are also blocking the availability of mass market encryption software on the market today, which makes it hard to build security in these networks.

I think that if Congress is going to take these issues on, privacy and law enforcement, in a legislative arena, then all of those issues should be on the table and we should look for a solution which really does not let these become segmented off into different portions, but that we look at those three issues related together.

Senator SPECTER. I am going to conclude with just a brief statement, less than a minute, and I know Chairman Edwards has time commitments and pressures, and I want to thank my colleagues for deferring to me. I found the hearing to be most useful, as the complexity of the problem is enormous. I do not want the Attorney General at the head of industrial policy, at all which is your statement. I do not want an industrial policy. I want to continue with the free enterprise system and a balancing of law enforcement interests and privacy interests. When the crunch comes, we have always chosen privacy as the superior value in our country, and I think that has to be maintained. But within that context of that value, we have to do what we can for law enforcement.

I think we are prepared to do the work on it. Senator Leahy has had a lot of experience on evaluating probable cause and mere suspicion and stop at risk, and so have some of the rest of us. Thank you very much.

Senator LEAHY. Thank you, Arlen.

Mr. Chairman?

Representative EDWARDS. Thank you, Senator Leahy. This is a very useful hearing, if just to frighten us to death, because the problem is rather awesome.

I have a nuts-and-bolts question for you, Mr. Neel. The Director said that he had 91 instances where the FBI did run into trouble that caused them some difficulty in wiretapping because of the advancements in technology. Do you know about those?

Mr. NEEL. We do not know specifically about those, and, in fact, up until just a few days ago, we had no evidence of these. Now, it may be semantics. It may very well be that the Agency has had problems with capacity on cellular telephone services that we have talked about in the past, and the companies have moved to expand that capacity. There may have been some other technical issues that created a delay.

There have been disputes about compensation, but to my knowledge, or at least to our knowledge most recently, there have not been cases where a local telephone exchange has refused to comply with such a request.

Mr. PLESSER. May I jump in on that, Congressman?

Representative EDWARDS. Yes.

Mr. PLESSER. In the Freedom of Information Act requests that CPSR initiated we got the information from the FBI on Project Root Canal, there was no indication of 91 problems of capability. There is a capacity issue that has been raised in the telephone company areas, but I think as Senator Leahy said in his questioning, there is a difference between compliance and guarantee. As these issues start to grow—and CTIA, I know, will be in on Monday—the companies have a responsibility to comply with the law. There is no question about that. And the question that I am really—I represent PCS companies and other people in the field, and the idea that a lawyer, any lawyer in this country is advising a client to say that you do not have to respond to digital—you know, to law enforcement requests in a digital environment is just totally foreign to me. The PCS, by the way, is covered. There is forbearance, but they would be subject and covered in this area.

So I am not sure where that information comes from, and I am not sure where the incidents of noncompliance are. I am sure CPSR and others will put some more FOI requests in and see if we can get some more information on it. But at this point I am not sure that we have had the basis to be able to evaluate what those 91 are.

Mr. BERMAN. I have for the record to submit CPSR FOI requests, Operation Root Canal, which essentially asked for incidents of failure to—you know, difficulty with law enforcement, and there were no difficulties. And we have been in a whole year dialog with the Clinton administration to expand on the record and give us instances so that industry could address these issues, and this coalition has been anxious to work with the FBI.

They have not given us 91 incidents. Those are new to us. And so it is a mystery why we have not been able to expand on the cooperative efforts and we are back here with a legislative effort that is far too sweeping.

Representative EDWARDS. Well, I think that I can speak for both the Senators and for the House members. We certainly have every intention of holding your feet to the fire, both sides. You know, total security is probably not possible. It would be possible, but we would not want to live in that kind of a society. So we do have to balance that.

Mr. PLESSER. There is not a policy dispute here. There is not a policy dispute about the fact that the FBI or other law enforcement should be able to get access to digital communications through title III warrants. There is not a policy dispute. There is a technology solutions dispute. There is a dispute as to whether the solution is really appropriate in the proposed legislation, whether or not it has the normal boundaries legislation should normally have, and whether or not it identifies the solutions. The technical case has not been made. No one is arguing with the policy case.

Representative EDWARDS. Have you a written proposal, or have you talked to the telephone companies about your idea of a compromise, Mr. Berman?

Mr. BERMAN. The Berman compromise. I think that before moving to legislation that structures a whole set of band-aids, it would be better to perhaps go back and look at why this informal process is not working. In other words, maybe there are not enough people at the table. Maybe it needs to be that there—you know, if it took the FBI a long time to figure out that call forwarding was a problem, if there had been an ongoing dialog about what new technologies were being developed and they had input from the industry, the might have been aware of the problem and worked cooperatively with industry towards a solution much sooner. And I do not think that you can just limit that to the telephone industry because it is the cable industry and it is the computer industry. But rather than putting a big stick on top of them with fines and injunctions, perhaps a Federal advisory board or a more structured process for looking at these issues over a period of time with reporting back to Congress and everybody keeping everybody's foot to the fire and trying to identify problems and create a process for working on these might be a better solution than going this far towards an industrial policy approach.

Representative EDWARDS. I think your bringing up the matter of the NCIC is timely because historically we have had to watch the development of the NCIC, while encouraging it as a very valuable law enforcement tool, to make sure that it does not become a Big Brother. And with all the requests for involvement in the NCIC, I think we have kept it relatively pure, although we have had some defeats where it is being used for non-law-enforcement purposes. So I think that as a model, we do need the——

Mr. BERMAN. We did bring together—and you have brought together—experts from different parts of industry, the computer industry, law enforcement, privacy, and they have worked together. I think in many ways the industry is moving to try and meet the standards of the FBI in terms of software design and hardware design, and I think that from a privacy point of view, privacy interests ought to be represented at that table as they discuss those requirements even outside of legislation so that there is a process which is weighing these issues as the technology is developed and deployed and comes out of the shop.

Maybe Congress can do some very narrow surgical legislation that creates a process which, you know, if it does not work, then you can come back and escalate. But to go from informal process and, geez, we have had some problems and we have 91 incidents, but some of them have been solved and we have this contest about who did what, and then to move on this kind of legislation or to try and set requirements—I mean, Senator Specter, with all due respect, knowing what the FBI is saying, you meet our requirements for cellular ports, capacity and capability, well, how does the—if the FBI cannot tell industry what the requirements are, how much they are going to need, it is hard to build.

Mr. PLESSER. But it is not even that. This legislation, the way it is written, does not require them to say what they need. When they come around to it, if they do not have it, then they are going to be penalized. It requires a guarantee rather than compliance. There is no standard. As a lawyer advising a company, how do you advise what you have to do to comply? This legislation does not set that up. This legislation says if in the end you cannot do what we want, we are going to hit you.

There is no way to resolve it, and I think there is a lot of middle ground that can be looked at.

Mr. NEEL. Mr. Chairman, if I may add to that, I think it is important to point out that the telephone industry in particular—in fact, I think the entire communications industry—has absolutely no incentive to not cooperate with law enforcement on this issue. The fact that the process has not borne fruit in the way that the Director would have hoped is more of an indicator of just how tough the problem is, not that the parties involved, certainly the telephone industry, are intransigent somehow, in some respect, in finding that solution.

Representative EDWARDS. I find all your testimony hopeful, and I think that we have work to do, Mr. Chairman. I would yield.

Senator LEAHY. Thank you very much.

As I sit here listening to this, I realize that we are not that far from a time when I am going to be able to sit at home, make telephone calls to my children in college, use the same lines to balance my checkbook, and either withdraw money or send it on to pay bills, order videos, probably move my medical records back and forth or get the results of a medical exam or set up appointments for another.

Frankly, I do not want anybody to be able to go in and nose around in all that any more than I would want anyone to open my mail if the videos were being mailed to me or if my doctor was sending my latest cholesterol reports. Actually, I would be willing to do that because they are very good. That is about the only thing in this aging body that is.

But there is another part that frightens the hell out of me, and that is letting the U.S. Government determine where our technology goes, especially in telecommunications. The highlight of the U.S. Government's telecommunications has been our military and the White House communication system. These systems have been decades behind what is available at Radio Shack to buy. We have ships that are side by side that cannot talk to each other.

The much-vaunted telecommunications system at the White House, up until the very recent time, worked only because you had about 20 times more people than anybody in their right mind would ever have to run anything. Up to just about a year ago they still used a phone system where you plugged in wires to make conections. This is the sort of system advertised back in the 1940's, and in the 1950's and 1960's went into the Smithsonian. Had they not been able to find another one, they could have gone to the White House and gotten it.

We spend billions in communications for the military. Most people in industry buy off the shelf far, far better equipment that works quicker, better, and is more versatile. In Desert Storm, after the millions we put into our military communications systems, what really worked is when somebody just went and got off the shelf a cellular phone system. That is the one thing that they could be sure of working. But the stuff they had that had been designed and superdesigned and refined would not work. And I am concerned about a situation where the Department of Justice is going to sign off on this. My gosh, the Department of Justice is not filling second-, third-, or fourth-level positions a year or so into a new administration. Nothing against this particular Department of Justice; it happens in most of them. Can you imagine them signing off on new technology, determining whether you are going to have this phone system or a new one? We would still be back with rotary telephones. Bring back the princess phone.

If we thought the old AT&T was stodgy and behind the times, which, of course, it was because they had a monopoly, can you imagine what it would be like if you have some study committee at the Department of Justice determining whether with 40 or 50 or 60 or 100 different telecommunications companies or high-tech companies, whether a particular technology could go forward?

So I am concerned by that idea, and I do not think, in credit to the FBI, that is really what anybody wants. But I am afraid that may be the result. If we do that, you are going to find people going to Sweden, Germany, and everywhere else to buy their communications systems because we will have fallen behind, just as we did back when we had a monopolistic phone company because there was no incentive to move forward.

Mr. NEEL. Mr. Chairman, I would point out one thing. You mentioned the backward nature of the White House telephone system. I can tell you from personal knowledge that the reason that system exists is because they felt like they could not afford to put in a state-of-the-art telephone system. When I was there, I had a telephone that was in the same office during the Nixon administration, and if the White House cannot afford to upgrade its telephone system, it is hard to imagine the Department of Justice coming up with many billions of dollars to authorize the increased capability envisioned in this proposal.

Senator LEAHY. Let's go back to another point, though. Are the telephone companies trying to deny the FBI this technology? Do you know of any phone companies that are saying let's build our switching systems this way so the FBI or the State police or whomever else under proper court order cannot get in here?

Mr. NEEL. No, absolutely not. As I said, there would not be any incentive for doing that. It would be a huge public relations outcry, frankly, if you were to do that. But I would point out one thing: By exempting a broad range of technologies, as this proposal has done, you will create an incentive for very sophisticated criminals to buy and deploy technology that will evade this kind of system.

Senator LEAHY. This does have large exemptions.

Mr. NEEL. Yes, absolutely.

Senator LEAHY. Now, phone companies have to isolate particular lines for both billing and maintenance purposes, do they not? It does not make any difference whether they are digital or analog?

Mr. NEEL. I believe that is correct.

Senator LEAHY. Then I would raise the question—and you can submit your answer on this for the record if you would like—why that same technology could not be used for wiretap capability, assuming it could. Let me ask this question: If you have to isolate digital or analog lines for both maintenance and billing purposes, do you know of anybody within the telephone companies who, if told that they could use that same technology for wiretap purposes, would be opposed to that?

Mr. NEEL. I do not believe so. We will certainly get further information about that and get it to you. But I do not believe that is the case.

Mr. PLESSER. Senator, from our research this last summer, the implication was that that was really the best protection for wiretap information, is that, in fact, companies do have to maintain isolated bit streams for billing and maintenance purposes, and it is essentially through those paths that wiretaps are made, and I think those are continuing in digital.

Senator LEAHY. Are there services in the present systems that are untappable?

Mr. NEEL. In the present system, I believe not.

Senator LEAHY. Are there features or services being planned that would be untappable?

Mr. NEEL. I cannot speak for the literally thousands of companies that have new services technology on the drawing board. I do not know the answer to that question. There may very well be some entrepreneur somewhere who is brilliantly designing a piece of equipment who would have no reason to know what the FBI may or may not want in the future. So it would be almost impossible to know that.

Senator LEAHY. There are over a thousand digital switches in use in the Unites States today. Do you know if any interception orders were served on any of these switches?

Mr. NEEL. Orders for failure to comply?

Senator LEAHY. No, were any interception orders conducted on facilities using these digital switches? Is that done?

Mr. NEEL. Oh, yes.

Mr. PLESSER. All the time.

Mr. NEEL. That is commonplace.

Senator LEAHY. And have there been problems with those orders?

Mr. NEEL. Not to my knowledge. Other than, as I mentioned earlier, some possible delays to solve interim problems and these capacity issues that do not go to the issue of whether it is digital or analog, I do not believe so.

Senator LEAHY. Speed dialing, call forwarding, do those services make wiretapping difficult, if not impossible?

Mr. NEEL. Well, we do not know if it makes it impossible. Clearly what we do know is that the technical problem related to call forwarding can be alleviated through a new switch that would allow the FBI to monitor the calls from the switch, and we are working to make sure that that technology is made available.

As I mentioned earlier, the software upgrade for that alone would cost nearly $2 billion, so we are working on that, and call forwarding has been cited as a problem now and in the future, and we think there is a fix underway.

Senator LEAHY. Under this proposal, whatever the cost of that fix was, would the U.S. taxpayers pay for that?

Mr. NEEL. I believe that is correct.

Senator LEAHY. Had this proposal been in place when call forwarding and speed dialing were first designed, would the industry have had to hold back from marketing them until a wiretap solution was found?

Mr. NEEL. Well, I cannot imagine that any company considering the deployment of new product or service that could be facing a $10,000 fine, much less the kind of public humiliation that would be involved here, deploying this technology until the Justice Department certified it.

Senator LEAHY. You mean I would have to learn my telephone numbers all over again? I couldn't just hit line 5 for a particular phone number?

Mr. BERMAN. Excuse me, Senator. I mean, it is important to look back at the last draft. While they have changed the bill to make it less controversial, they did have a certification process, one before the FCC and the second before the Attorney General. So the specter of having the telecommunications industry taking its products into the Justice Department and going through a clearance process, whether that is a PBX system or something going on with the Internet or a new computer chip, it was really there. And, in fact, even though this bill is drafted politically to cover only common carriers, many of the problems cannot be solved without bringing other people to the table, because the telephone company is not in the position always to be the most reasonable place to go to get the communications.

Senator LEAHY. I want to yield to Mr. Canady, but the concern I have is more of an anecdotal one. After 20 years of dealing directly with the Federal Government, both its civilian and military parts, I have never seen any organization that has so consistently, so doggedly, and with such expertise, stayed behind the curve on telecommunications as the Federal Government. They have raised it to an art form. I would be very concerned to see the Government in a position of determining how the rest of us move into the 21st century.

Mr. Canady?

Representative CANADY. Thank you, Mr. Chairman.

I want to thank each of you for your testimony. It has been very interesting, and I think it highlights for us how complex an issue we are dealing with here.

I will tell you that I am a little uncertain about whether you think there is a problem for law enforcement or not. There were discussions, indications in the testimony early on that at that point led me to believe that you thought there was a problem for law enforcement and that at a certain point it might be difficult for you to comply with the requests that they would make as they have made in the past.

Then we hear the indication that these access points for individual customers will still be there, and you will be able to tap into those as you have in the past. I just want to see, for me and for the other members here, if we can get a better fix on whether you think there is going to be a problem for law enforcement. I understand there is a special concern here about call forwarding, but putting that aside, looking at the other issues, what do you say to that?

Mr. NEEL. Well, we do not believe there is a problem right now, and, in fact, I think the Director reaffirmed that.

Representative CANADY. My question is not so much right now, because I understand—I think the key point we have to understand here is this is a rapidly changing technology. The world out there is moving very fast. We just spent time in the Judiciary Committee over in the House hopefully helping move that world forward in some of the things we are doing on legislation relating to telecommunications. But I think what we have to be concerned about is where this is moving, and I think that time is of the essence here because we need to make certain that we avoid problems that we can avoid and we avoid expenses that we can avoid.

I would prefer and I believe all of us would prefer for this to be worked out in the private sector without the need for additional legislation. But I am certainly and I believe the other members here are also concerned about maintaining the capability of law enforcement to get the information the way they have been getting information since 1968. And our goal is to ensure that that goes on without disruption for a significant period of time.

So don't just address the way things are now but the way things are going to be within the foreseeable future, given the technology that exists and that is going to be implemented.

Mr. PLESSER. May I just respond? Going back, 1968 was a different world. There was one telephone company. There was one person, one corporate entity that did everything. Today——

Representative CANADY. I do not know of a time when there was one telephone company.

Mr. PLESSER. Well, one primary telephone company, and a couple of smaller ones. Today, this is——

Representative CANADY. Well, I think that, quite frankly, does a little in justice to the entities such as General Telephone and United Telephone and others, but you can proceed.

Mr. PLESSER. Well, I was going back to 1968, and I did not mean to slight them.

There are a lot of people involved in telecommunications today. Part of the problem that I think the FBI is expressing is a concern that not everybody has maintenance ports available to each communications.

When I send a call to the west coast, it may be on one company; it may be on two or three companies. There may be a packet switching system. There may be other people carrying parts of that communication through different pipes.

The issue addressed by this legislation and I think the concern——

Representative CANADY. OK, I do not think you are answering my question.

Mr. PLESSER. No, I am agreeing with you, actually.

Representative CANADY. If you would not mind, let me ask Mr. Neel to address my question and Mr. Berman to address my question, the people who have testified, and I will be happy for you to make your comments.

Mr. NEEL. Congressman, since there are new products and services being envisioned on drawing boards, about to be deployed, potential future technologies, no one knows what the potential problems would be for law enforcement in wiretapping. That——

Representative CANADY. Well, let me ask you, though. We know about technologies that are there and that are planned for implementation. OK? People have plans. And I understand from the testimony of the Director that he has been told by people in the industry that a couple of years down the road we are not going to be able to comply with requests that will be made at that time given the technology and the devices that will be used at that point. Is that true or not true?

Mr. NEEL. Well, I do not know the specifics of what he is referring to, and he referred to, you know, telephone company lawyers and lawyers tend to be extremely precise in not guaranteeing things. But the point is this is what the Quantico Group is exactly trying to establish right now, what those problems will be and how we address them.

Frankly, even if this proposal were to become law, it would not fix the problem. You cannot wave a magic wand and say it is done.

Representative CANADY. Right I understand that, and——

Mr. BERMAN. Let me answer the question.

Representative CANADY. Sure.

Mr. BERMAN. There are going to be problems. There are problems. We are going from, you know, AT&T and Ma Bell. We are splitting into a network of networks. And what is running over the Internet is 40,000 different networks. That is running over the telephone lines which the telephone company does not control. There are cable networks that are going to be in the telephone business. That is a new kind of network. There are wireless networks. There is enormous diversity, and communications are going to be carried by many kinds of providers, not just common carriers but all kinds of providers. And so there is complexity out there of where in the stream do you go and where is the most reasonable place to impose responsibilities, and are those technical, are they legal and so forth.

That is why I think it underscores that the FBI has a problem, but it does not support a legislative proposal that says let's try and fix it for all time in some sort of industrial policy that says we want to control where all these networks are going, but rather suggests that the FBI has to come up to speed and learn a lot more about where network technology is and get in a much clearer dialog with the new computer and communications industry as they develop products and figure out solutions. I think that is the way to go, and it is not to put a big baseball bat or the power of the State in the hands of the FBI or the Attorney General.

Representative CANADY. On that point, I agree with the thrust of what you are saying. I think this is something that requires dialog, and that obviously is a two-way street. But given the complexity of the situation, given the multitude of entities that are involved, I am not at all certain that this is something that can be worked out by the FBI sitting down at the table with some people and coming to an agreement. I think that the complexity that you have described actually indicates that that type of solution may not be possible and that some type of legislation may be required to bring that dialog to a focus so that we can make policy decisions about how this is going to be addressed. It may not be the legislation that the FBI has submitted at this point, and I am certainly not wedded to that.

Mr. NEEL. Congressman, we would support giving teeth to the Quantico process that is in place right now. That could be one solution here. Also, let me point out that you are exactly right, there have been over 1,100 independent and small telephone companies for many decades, even when there was just Ma Bell, and they have been complying with wiretap requests as well. But the prospective problems that could exist in this network would be a little bit like saying, well, where is war going to break out next? You do not deploy enormous armies in 500 points across the world to prevent the potential of an outbreak somewhere. To a certain extent, this proposal says, well, we do not know exactly what the problem will be and we really cannot tell you exactly what specific technical standard we want you to comply to, we just want to make sure you will do it whenever we want it. And it is a little bit like using a hammer when a small wrench is really what is required.

Representative CANADY. I understand your concerns with that, and I think that is a legitimate concern. I believe our task is to try to focus on what the problem is and the ways that we can come up with defining standards that are workable, that you can be expected to meet, and that will still ensure that law enforcement gets the information that is needed.

I have taken longer than I should have.

Mr. BERMAN. Can I just amend——

Representative CANADY. Yes.

Mr. BERMAN. That we make sure that when we are engaged in this process, that we look at, in this network of networks, we also have privacy, confidentiality, and security problems of major proportions which need to be addressed, and they need to be addressed in the same technical and dialog between industry, government, private sector, public interest, Congress, that has to go together, that it is not a one-sided effort, that we are trying to keep the balance that Congress struck when it passed the Electronic Communications Privacy Act in 1986, which recognized a new era of communications. If we have to add to that and in a process that keeps everyone up to date, both on the privacy threats and on law enforcement threats, let's add that process and address all those issues at the same time.

Representative CANADY. Well, I think it is important that we do that, and I will just conclude by thanking each of you for your testimony. It has been very helpful. This is something that is going to require a lot of work by all of those who have an interest in this, and I certainly will look forward to working with you to come up with something that will protect all the things that we are seeking to protect—privacy, the ability of law enforcement, and also the vitality of our free enterprise system in telecommunications—because all of those are critical things that concern us.

Senator LEAHY. Senator Cohen?

Senator COHEN. Thank you, Mr. Chairman, and thank you for allowing me to sit in on this hearing. I am not a member of this subcommittee, but I do have an interest in the subject matter.

Senator LEAHY. We are delighted to have you here and delighted to have your expertise.

Senator COHEN. One of the real threats that we are worried about is big-brotherism. You can have Big Brother in the private sector as well as in the public sector. We are mesmerized by technology. We are climbing Jacob's ladder into a technological stratosphere, and we are simply overwhelmed and intrigued with the potential of what we are capable of achieving, without much concern about what it is doing to some old and cherished values. While listening to your testimony, I recalled that a manufacturer had devised an instrument you could put on your television set. The moment you walked into the room, the instrument started to view you. The purpose of it was to monitor the habits of individuals as they were watching television to determine human reaction to what is on the television.

Some advertising firms were then sponsoring the idea, and it struck me that we are inching closer and closer to "1984."

You can have a step toward big brotherism in the private sector where there are no rules, and you can have a step toward it, of course, in the public sector where hopefully we will always try to strike the balance between the need for privacy and what Senator Leahy said in his written statement about the need to protect our citizens against various threats.

My understanding is that it is not the purpose of the Bureau or the intelligence community to dictate the standards of technology, but to ensure that law enforcement walks in locked step with technology so that we maintain at least the status quo, that we do not find the FBI rushing from several hundred yards back trying to catch up constantly.

One of the great ironies of our society is that we always look back in retroactive nostalgia for what the Agency supposed to do at that time. I recall, for example, when a DC–10 dropped an engine over Chicago. The first cry was, where was the FAA? Then we had Love Canal, where was the EPA? On Three Mile Island, where was the Nuclear Regulatory Commission? We always tend to look back and ask, where were the agencies that we thought were protecting us?

Senator Leahy mentioned the Trade Center in his opening remarks. I recall during the Persian Gulf conflict that there was widespread fear in this country that we were going to be faced with an ignition of certain cells that were sleeping in this country, and that people would be dropping biological and chemical weapons into water supplies. What was the FBI capable of at that time?

We tend to place a higher premium on our rights of privacy until a tragedy strikes and then we say, where were our law enforcement officials? It is always a delicate balance. How do we strike the right kind of balance? We have tried to strike that balance with current technology. I am not aware that the FBI has made an intrusive, widespread violation into the realm of privacy that is not justifiable. There are certain procedures they have to follow. They have to go to the court. That is not an easy thing to do. They have to report that to an administrative council and so forth.

I don't want to seem to be ignoring the need for privacy. My own belief is we are going to find ourselves in a society in the future in which you will have an increase in the level of terrorism, not only abroad but here in the United States. That will call into question the tension that normally exists between the need for privacy and the need for protection, and it will shift from time to time depending upon the horrific nature of the latest attack upon our citizens.

The FBI needs to try to maintain at least a status quo position, where they are today, fearing where technology is going tomorrow. Frankly, I am not sure that just because something is possible it is necessarily desirable in terms of preserving our values. Technology can achieve untold things, but maybe they are inconsistent with cherished values that we have had.

That is a decision that we do not make at the governmental level. That is something that we have to try to continue to educate ourselves on. Just because we can achieve it, does it mean we should desire it?

One of the fears of the Agency would be that we now have an informal arrangement. Mr. Berman, you talked about an informal arrangement, that we have ongoing talks. But these, I assume, are voluntary by the companies who are involved. I am not sure how committees work in your business, but I suspect they work like the ones here. Sometimes people show up and sometimes they do not. It is periodic at best. There may be a few members who are very conscientious. There may be a few members who say they are not interested in helping our law enforcement agencies.

As the race for superiority in technology continues to escalate, there will be some firms that say, we do not want to be a part of this, we got a better deal than AT&T or whatever the firm might be, and we can get there faster and not comply with what these responsible firms are trying to do to accommodate law enforcement's needs. These firms will also say, we want to get there first, we want to get there fast, and we want to make the biggest amount of money; and if we can market this domestically and internationally, that is what we are going to do, and to hell with the FBI and law enforcement.

There may be a need for legislation in some form. I am not sure it is this specifically, but I would not dismiss it out of hand by saying we can operate informally. We may need to have an adjustment. The legislation must neither hamper technological breakthroughs nor intrude in a way that is undesirable in the view of most of the American public.

Mr. BERMAN. We have suggested the possibility of a more formal process with more diversity than simply the telephone industry, the computer industry, Internet, and that process could go on, and, in fact, it would be encouraging the FBI to catch up with the technology. I am not saying that they are behind or are Luddites, but to really create a process that makes that an ongoing dialog that is less than informal.

That is different and I think far more acceptable than saying stop the world, you know, we have got to get off here because we could lose control.

Senator COHEN. Technology, like time, cannot be stuffed in a bottle. We must recognize that. The real issue is: Can a system be devised where the law enforcement agencies are running in tandem with technology to make sure that technology is not racing ahead so fast that law enforcement is put at such a severe disadvantage that it cannot fulfill its mission of protecting the American people? Further, can we devise such system in a way that does not unduly intrude into the value we place on privacy? Obviously, whenever we allow the FBI or any other agency to intrude, we knowingly give up some of our privacy. We are very conscious of this, and do not do this lightheartedly.

Mr. BERMAN. We are for that process, but we have to be on guard on privacy grounds. This legislation, as it was drafted, would do some very interesting things to communications. It would permit the FBI to move a communication to a remote location and pick it up and require networks design that. Now, that may be the future, but also it would have made Watergate really hard to uncover if you could have moved the communication from the Howard Johnson's Hotel to some remote site and no one was ever able to trace that interception.

Senator COHEN. I do not think that is how Watergate was broken. That is another matter altogether.

Senator LEAHY. Nor do I think that will determine which way this committee goes.

Mr. NEEL. Senator, I would respond to one thing. In terms of the willingness of the private companies participating in this forum, the entire local telephone industry is represented at those meetings, and my information is that participation in that work has been enthusiastic and that attendance is universal. I do not think our industry would have any problems with sterner mandates for participation in that process.

Senator COHEN. Mr. Chairman, thank you very much. I hope to be able to continue to participate.

Senator LEAHY. I appreciate your participation, and I appreciate the help not only because of our own personal friendship but because of your diligence on this committee and your experience in this area.

Nobody is suggesting we do away with our wiretap legislation; certainly I am not. But even if we can wiretap messages transmitted over telephone lines or the air waves if it is cellular, if that message is encrypted, law enforcement might still not have anything. I realize we are talking about an issue that is going to be before this subcommittee in another forum, but if person A is saying to person B something that is encrypted with an unbreakable code, even if you can pick it up, even if you can access it with a wiretap, you still have nothing except meaningless noises.

Mr. NEEL. That is correct, and clearly that represents a challenge to law enforcement and to the Government to determine the degrees to which encryption should be——

Senator LEAHY. The reason I raise the point is that even if we make sure that whatever is being sent can be tapped, you still have a second problem if the person sending the message encrypts it. You still have nothing.

Mr. NEEL. That is correct.

Senator LEAHY. Now, I might say on the question of this cooperative endeavor—and I want to send this message out very clearly—I would encourage industry and law enforcement to continue this cooperative effort. But I am not prepared to support a government veto on telecommunication technology advances, for a couple of reasons. One, the Federal Government has historically stayed way behind the curve on telecommunications and, for that matter, computer technology. In a lot of areas, both military and civilian, where the Federal Government should be doing much better, an outrageous amount of time and effort and money has probably been wasted because we have stayed so far behind the curve.

Also, I am not going to hinder one of the areas where the United States has been such a great leader while government officials try to make up their mind how far we want them to be leaders. So I would urge everybody to work on the cooperation, but I would suggest that legislation allowing government vetoes on technological advances by the best innovative minds in America is not going to occur.

Incidentally, the FBI Director estimated the cost to be about $500 million over the next 3 years to make existing equipment and systems wiretap-friendly. You say about $1.8 billion.

Mr. NEEL. I said we think it will cost $1.8 billion to solve only one part of the call forwarding issue alone, not to mention any other costs incurred through this. So we think it would be many multiples of the figure that the FBI cited.

Senator LEAHY. In the Quantico Committee, are the huge differences in cost estimates an issue that is being discussed?

Mr. NEEL. Yes, I believe it is. Surely cost is a main point of interest out there.

Senator LEAHY. Because if these costs get up high enough, you have probably got a moot point facing us to begin with.

Mr. NEEL. Well, as I mentioned earlier, no one wants to put a price tag on the fight against crime, and our industry is——

Senator LEAHY. We do it all the time. [Laughter.]

Mr. NEEL. Well, our industry would not want to do that in terms of deciding whether it is worth the Government's spending that kind of money. But we do think that it is important that you have realistic numbers to know what the taxpayer exposure will be if you were to implement a proposal such as this.

Senator LEAHY. Let me close with this on needs of law enforcement. I would say this to the industry to add to your incentive to work very closely on this. This is not just a question of finding out where the guy who held up the branch bank might be stashing the $50,000, but it could very, very well be a question of finding the person who is going to blow up an airplane as it is landing at Kennedy Airport, or the person who is going to blow up a convention center with 2,000, 3,000 or 100,000 people in it to make some political point dealing with concerns in a country that most Americans may not even have heard about.

These are the kinds of crimes possible in an era when transportation is so easy and where the weapons of devastation that can be used by terrorists are way beyond anything anybody thought of when the first wiretapping was being done. So the stakes are very, very high for our own security. I have said over and over again that a well-concentrated terrorist act poses danger to our constitutional liberties that we have relied on in our democracy for 200 years. A dozen well-equipped, motivated, and financed terrorists can pose more threat to our democratic liberties in this country than all the armies arrayed against us in world wars throughout this century.

Representative EDWARDS. I would like to point out that the FBI has done a remarkably successful job in combatting terrorism in this country. We have kept a careful count of it in my subcommittee. Fifteen years ago, there were several hundred incidents per year, and now it is down to a handful each year. I am going to be very interested in our exploring what the other friendly countries are doing about this because they really have a lot of terrorism that puts ours to shame. Monthly, in Europe there are terrorist incidents. So they must have the same concerns that we have. But I say I have great confidence in what our sister subcommittee in the Senate is going to do. I am really honored that we can work together because this is a very difficult problem, Mr. Chairman.

Senator LEAHY. It is, indeed.

Gentlemen, thank you very, very much.

Mr. BERMAN. Thank you. The coalition of 50 organizations really, the cross-communication, is very anxious to work with the committee and the administration to find a way out of this and to find a solution that balances these values.

Senator LEAHY. Let me tell you, nobody is more anxious to have you work closely together and find a solution than I am, because I must say that if we have to design a legislative solution today that will predict what technology will be 5 or 6 years from now, it is not going to work. It would be inadequate for industry and I am afraid it would be inadequate for law enforcement. It would end up being a lose/lose situation, and we do not want that.

Mr. NEEL. Thank you very much.

Mr. BERMAN. Thank you very much.

Senator LEAHY. Our last witness is William C. O'Malley of the National District Attorneys Association. We thought that this would be a good name to have this close to St. Patrick's Day.

Also, as I mentioned to Senator Specter earlier, I am a former vice president of the National District Attorneys Association, back in the distant past. I must say, Mr. Chairman, I gave up the honor and glory of becoming president of that association, which I would have had in another year or year-and-a-half, for the anonymity of the U.S. Senate. And for the last 20 years, I am not sure I made the right choice because the most enjoyable job in government I have ever had was as a prosecutor.

Representative EDWARDS. From our point of view, you made the right choice because we could not have gotten along without you.

Senator LEAHY. I do not know about that, but I thank you very much.

Mr. O'Malley?

Mr. O'MALLEY. I will say that we will miss your leadership, too, Mr. Chairman.

Representative EDWARDS. Thank you.

STATEMENT OF WILLIAM C. O'MALLEY, DISTRICT ATTORNEY FOR PLYMOUTH COUNTY, MA, AND PRESIDENT, NATIONAL DISTRICT ATTORNEYS ASSOCIATION

Mr. O'MALLEY. My name is Bill O'Malley. I live in Brockton, MA. I am the district attorney of Plymouth County, 26 towns and 1 city just south of Boston. I have been a prosecutor for 22 years. I am the president of the National District Attorneys Association, an organization with 7,000 members who represent prosecutors of this country.

I will begin by pointing out that State and local prosecutors perform more than half of all the wiretaps. Approximately 60 percent of the some 850 wiretaps that are authorized in the course of the average year are conducted by district attorneys or State attorneys.

In the time I have been a prosecutor, I have personally applied for as district attorney or conducted as an assistant district attorney 25 wiretaps. They have been focused in the area of organized crime, illegal gaming, and loan sharking primarily, and for the past 10 years exclusively in the area of drug investigations.

The only tool that permits us to get above the retail level in the chain of distribution of illegal drugs and to get the people who bring drugs into this country, who finance at the wholesale level the purveying of illegal drugs, is the tool of wiretapping.

In July 1992, our board of directors unanimously passed a resolution supporting legislation that is designed to ensure that law enforcement agencies retain the capability of performing court-authorized electronic surveillance in light of changes in the technology. I think that it is critically important to understand what Congress did in 1968 when it addressed the issue of balancing privacy on the one hand and an effective tool for law enforcement on the other. And the safeguards that were put in place are such that the average person is shocked to learn that there are only some 800 to 900 wiretaps in the course of a year and that that includes every Federal agency, every State attorney general's office, and every local prosecutor, between 800 and 900 a year.

The amount of paperwork that is required to satisfy the formal requirements of title 18, title III, and the State laws runs between 25 and 200 pages. There are three kinds of probable cause that must be shown before a wiretap order can be issued. The States are permitted in our Federal system to grant greater protection of rights of our citizens. They are not allowed to grant greater authority to law enforcement. Congress preempted the field. We are now, because technology is changing, revisiting issues that have been very carefully balanced some 25 years ago. It is this simple. With 1,500-some companies providing services and equipment in the telecommunication area, voluntary agreement will never preserve our capabilities of carrying out the authority give to us 25 years ago.

We are in the process of losing that. We are in jeopardy of losing that authority. All we seek is retention of the authority that has already been granted and, frankly, has been proven very, very effective in the intervening 25 years.

We look to Congress for leadership. We need your leadership. The alternative is to go to court to seek to enforce the requirement under current law that certain facilities and services be granted. I have had occasion one time where I had information through a State trooper who worked for me from an engineer for the phone company that a certain kind of information could be given to me. I specified that I wanted that provided. The phone company denied that it was technically capable of doing that.

I petitioned the court to hold the phone company in contempt. It took me 3 months of litigation to ultimately get an order compelling the company to provide that service. It was a cross-frame unit trap. The phone company did give me the——

Senator LEAHY. What kind of trap?

Mr. O'MALLEY. Cross-frame unit trap. I had two switching stations in one municipality. Tapping a line, I could identify all outgoing calls. I could not identify the source of incoming calls. The phone company had the ability to give me that. They denied it. I compelled it. It ended up being worthless by the time I ultimately got that after 3 months of litigation.

I see the red light. I am happy to answer any questions that you have. I will tell you that all we want is the tools that we have had for 25 years that we have used very responsibly and very effectively for 25 years, and that is all we are looking for.

Senator LEAHY. You understand, Mr. O'Malley, that we want to continue those tools. There is nobody on these committees who is opposed to wiretaps continuing as we have used them. I think those of us who have had experience with them from a law enforcement point of view understand the two things that you stressed: one, their usefulness, but, second, that you go through an awful lot of hoops before you are even allowed to get the court order. It is not a case that we sometimes see on the TV program where somebody says, oh, yes, tap that phone, you know, and somebody runs out and taps it. There is a lot more that goes into it, everything from the probable cause showings on through.

Mr. O'MALLEY. That is right, Chairman Leahy. But I would point out that because of change in technology, actually several different changes in technology but primarily the change from an analog system to a digital system, we are losing the ability to effectuate that authority.

Senator LEAHY. Have you had experience of not being able to get a tap because of digital?

Mr. O'MALLEY. I have not. Plymouth County has not yet gone to optical fiber, ISDN, or some of the new technologies. But I have heard from district attorneys around this country that they have had that problem.

Senator LEAHY. The cross trap that you used, was that digital?

Mr. O'MALLEY. No, it was not. It was hard wire, copper wire, twisted cable, coaxial.

Senator LEAHY. So the concern there was the noncooperation by the telephone company?

Mr. O'MALLEY. The phone company is concerned with public relations, frankly. Four years ago discussions began. We have just been told it is going to cost a billion dollars to deal with the needs of call forwarding. Four years have gone by. Where is the help? We cannot get all the players at a table. There is no table big enough to bring all the people who must be involved.

If I could just make one last comment?

Senator LEAHY. Sure.

Mr. O'MALLEY. We do not want the Attorney General or the Department of Justice to be a policy regulator for industry in any way. I value and somewhat understand the emerging technologies, and I know how vitally important they are to the economy and in so many other ways in this country. It is like the law of the independent contractor. We rely on their demonstrated expertise. We tell them that we want a certain result, and the result we want is continued access to court-authorized interception. But we leave the means to them. They can comply with that result in any way that they choose, and, frankly, with all the different technologies that are involved, different solutions must be had. And it is impossible to prescribe with any particularity the means of achieving that access or maintaining that access.

Senator LEAHY. What you want is if you have a case where you can get a court order for a wiretap, you just want to execute it.

Mr. O'MALLEY. That is all we are looking for.

Senator LEAHY. You do not care whether you put it on the fifth floor or the first floor, the green box, the red box, or the blue box. You just want the traffic off that tap.

Mr. O'MALLEY. We have always climbed the poles ourselves and made a physical connection, and with the bit streams and the binary flow of communication, rather than two pairs of copper wires that you can physically connect to, you must connect at the same point. Every telecommunication provider gathers information on who initiated a communication, to whom they communicated, how long it lasted, the date and the time, because they need that information for billing. They have the capability, and they do, in fact, get all of that information. It is at that point that we, because of changes in technology, now must look to make the interception.

In other words, instead of climbing a telephone pole, it has to be in the switching station because that is the only point at which a particular conversation is accessible.

Senator LEAHY. Do you know nationwide how many wiretaps have been conducted say in the last year or so on digital switches?

Mr. O'MALLEY. I do not. I understand that there have been particular problems in the Miami-Dade County area, and basically in the areas where the transfer away from the analog system to the digital system is most advanced, that is where the problems have been.

Senator LEAHY. Mr. Edwards?

Representative EDWARDS. Mr. O'Malley, thank you for your testimony. Your fears are prospective, though. You do not have the list except for that one rather stubborn company that just did not do what you wanted them to do, and you mentioned other district attorneys throughout the country who you believe are having current problems because of the advancement of technology in the telephone business.

Your fears are prospective as to what is going to happen next month or the month after or the month after, but your testimony is not that right now you are having problems.

Mr. O'MALLEY. I have not personally had problems. I listened to the Bureau. Of course, I am dealing with a very small geographical area, as each DA does. The Bureau deals with the whole country and with the state of advanced technology in every part of the country, and they tell us of problems right now.

Representative EDWARDS. Well, the Bureau said they had 91 problems, particular incidents, and the industry said they did not think they did have. So we do have a conflict, and that is one of the problems these two subcommittees are going to have, being prospective about something that is going to happen. The telephone companies say we will take care of it by negotiation, by the fact that we already are taking care of these problems, and competition and the free market system and our good will and our understanding of the seriousness of the matter will ensure that, without law, we are going to take care of the problem. And the FBI says, no, we fear that the sky is going to fall in, and the telephone companies say you are being Chicken Little.

Mr. O'MALLEY. Respectfully, it is not an issue of the sky falling. It is something because of the diversity and multiplicity of organizations involved, both in the industry, hardware and service providers, and in the law enforcement community. It is not something amenable to resolution through discussion. We are asking for your leadership.

Representative EDWARDS. Well, it would be very helpful if you could ask some of your members who are having current difficulties with the telephone companies because of this particular problem, not just because you are having an argument with them on something else. We would certainly like to hear about it.

Thank you very much.

Senator LEAHY. Mr. Canady?

Representative CANADY. Mr. O'Malley, we appreciate your being here, and we appreciate your perspective as a local prosecutor on this. One thing that is going to be very helpful to us is getting at this issue that you touched on when you talked about the ability of the companies to get information about where calls originate and where they are going for their billing purposes.

I am not sure I understand, if the companies are going to continue to have that ability, why we cannot also tap into that stream at the same point.

Mr. O'MALLEY. We can, Congressman Canady, if appropriate technical provisions for that are made. And they have not been made, and they are not being made. And every day that goes by, the cost of going back and retrofitting it increases, and that is the problem.

The point at which that access can be had, it cannot be had now without changes in the software. That is what this legislation would require.

Representative CANADY. That is really the crux of this issue, and I appreciate your comments on that. One thing I would say to followup on that, is that, I think that although we need to adequately consider all aspects of this very complicated proposal, this is a situation in which time is of the essence.

Mr. O'MALLEY. Yes, it is.

Representative CANADY. Because if we delay unnecessarily, I think we will find ourselves facing costs down the road that we could have avoided. So that is why I am very pleased that the two chairmen have decided to conduct this hearing, and I understand there will be a further hearing or further hearings. I believe it is important that we move forward with addressing this issue and bringing all the parties together to try to come up with something that will protect all the interests that we are dedicated to protecting, the interest in effective law enforcement, the interest in protecting privacy, which I think is a concern that has to be taken into account, and all of this.

Mr. O'MALLEY. We share that concern. We are concerned with that, too.

Representative CANADY. All of these things, as well as the concern about protecting the ability of industry to move forward with technological innovation that will provide benefits to the consumers in this country. We need to make sure that anything that we structure does not unnecessarily impede technological innovation, which does provide us with so many benefits, and that is a very difficult balance that we are going to have to strike. But I think it is a task that we must undertake.

Thank you.

Senator LEAHY. Thank you, Mr. Canady.

Mr. O'Malley, when you are meeting either with the board of the NDAA or talking with your fellow prosecutors, tell them to please feel free to send on to me and I am sure to Chairman Edwards their own thoughts on this, areas where either they have had a real problem or an area where they found an innovative way of working around problems. We really would like to know. They should feel free to contact us and send the information on to us because I think, again, everybody here, from both bodies of Congress and both parties, wants to be able to meet the law enforcement needs that we have as a Nation, especially at a time when crime is becoming far more mobile, and far more complicated. Obviously we want to be able to have all the law enforcement tools necessary.

Mr. O'MALLEY. I will do that. I appreciate that. If I could end with one last short observation?

Senator LEAHY. Yes.

Mr. O'MALLEY. There has been a great deal of talk about privacy and a concern about access to increasing data that flows over the information highway. I would point out that right now, when I am with court authority intercepting a telephone communication, you may be talking to your doctor about your cholesterol, you may be talking to your minister or your priest or your rabbi, you may be talking to your banker or your attorney or anyone else, I am required by law right now to minimize the intrusion when a communication is nonincriminating. That is a requirement that I am held to, a very high standard, right now, and, of course, that would continue. And so the fact that a new technology will bring information of different kinds from one point to another on a different channel will not change the balance that this Congress struck in 1968.

I appreciate the chance to appear.

Senator LEAHY. That is a good point. I thank you for it.

Incidentally, I will include in the record a letter in support of new legislation from the National Sheriffs' Association and another one from the Federal Law Enforcement Officers Association.

[The letters follow:]

NATIONAL SHERIFF'S ASSOCIATION,
Alexandria, VA, March 15, 1994.

Hon. DON EDWARDS,
Subcommittee on Civil and Constitutional Rights,
Washington, DC.

DEAR CONGRESSMAN EDWARDS: On behalf of the 22,000 members of the National Sheriffs' (NSA), I am writing in support of proposed legislation that would preserve lawful telecommunications interceptions. As always, NSA is prepared to support legislation in the best interest of law enforcement and the public.

For your information, I have enclosed a copy of our resolution in support of digital telephony legislation. I would be most grateful if you would keep me informed.

Thank you for your endeavors and support of the nation's law enforcement community.

Sincerely,

CHARLES "BUD" MEEKS,
Executive Director.

1993-05

NATIONAL SHERIFFS' ASSOCIATION

Resolution

IN SUPPORT OF LEGISLATION TO ASSURE THE CAPABILITY OF LAW ENFORCEMENT TO CONTINUE TO ADMINISTER COURT-AUTHORIZED ELECTRONIC SURVEILLANCE

WHEREAS, the sheriffs are the chief law enforcement officials of their counties/cities and are dedicated to protecting and serving their constituents with increasingly greater demands to combat crime; and

WHEREAS, court-authorized electronic surveillance is a major investigative tool used by federal, state, and local law enforcement; and

WHEREAS, advances in the telecommunications industry are impeding the ability of law enforcement to effectively implement interception orders; and

WHEREAS, the National Sheriffs' Association supports proposed legislation that would preserve lawful telecommunications interceptions therefore maintaining the status quo; and

THEREFORE, BE IT RESOLVED that the National Sheriffs' Association urges the United States Congress to immediately enact legislation proposed by the Federal Bureau of Investigation which would clarify the duty of all telecommunications providers to ensure the ability of law enforcement to effectively continue to administer court-authorized intercepts.

Adopted at a meeting of the membership
This 23rd Day of June, 1993
Salt Lake City, Utah

FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION,
New York, NY, March 17, 1994.

Hon. PATRICK J. LEAHY,
Subcommittee on the Technology and the Law,
U.S. Senate, Washington, DC.

DEAR SENATOR LEAHY: On behalf of the over 8,000 men and woman of the Federal Law Enforcement Officers Association, I urge you to support the proposed legislation entitled the "Digital Telephony and Communications Privacy Improvement Act of 1994."

FLEOA recognizes that the privacy of all Americans is of the utmost importance and needs to be protected. Part of that protection is the responsibility of law enforcement, to ensure the safety and security of our communities. To accomplish this, law enforcement needs the ability to thoroughly investigate the criminal activities of those that threaten our nation's domestic and national security.

The current communications technology being developed must provide for warranted interception by law enforcement. To do otherwise would be inviting disaster. In a perfect world all of this would not be necessary. Unfortunately, terrorism and violent criminal gang activity is increasing.

Court authorized electronic monitoring by law enforcementis essential in the investigation of such crimes. The proposed legislation ensures that those providing electronic communication systems will have the technicalassistance necessary to accomplish court-authorized interception by law enforcement. The legislation would also establish the same ground rules throughout the industry that in turn would ensure competitive fairness between the providers.

Both law enforcement and the intelligence community have the responsibility for the safety and security of our nation. The providers of electronic communication systems should also bear a responsibility, to make available their systems for court-authorized interceptions. FLEOA urges the adoption and passage by Congress of the Digital Telephony and Communications Privacy Improvement Act of 1994.

Yours truly,

VICTOR OBOYSKI,
National President.

Senator LEAHY. Anything else?

Mr. O'MALLEY. Thank you very much.

[The prepared statement of Mr. O'Malley follows:]

PREPARED STATEMENT OF HON. WILLIAM C. O'MALLEY ON BEHALF OF THE NATIONAL DISTRICT ATTORNEY'S ASSOCIATION

On behalf of this country's elected prosecutors, I wish to thank you for this opportunity to voice our support for the Administration's proposed Digital Telephony and Communications Privacy Improvement Act of 1994. I am Bill O'Malley, District Attorney for Plymouth County, Massachusetts and have served the people of my county for 13 years. In addition I am proud to serve as the President of the National District Attorneys Association and am here to provide you with the views of that 7000 member organization.

In July 1992, the Board of Directors of our Association unanimously passed a resolution supporting legislation to assure that our law enforcement agencies retained the capability to perform court-authorized electronic surveillance in light of the emerging digital technologies. I am here to assure you that our members, elected to be in the forefront in our war against crime and terrorism, strongly adhere to our original resolution and its articulation in this Act.

Our national consciousness is evermore occupied by crime and its tragic aftermath. Poll-after-poll, survey-after-survey, reflect the fears and frustrations of the citizens who elected all of us to office. Now, you have the opportunity to either help answer those fears and frustrations or to add to them. If the law enforcement community does not have the opportunity to keep pace with advanced telecommunication technologies then the criminals who do have access to this technology will operate with impunity.

We are all continually amazed with the almost daily announcement of technological advances. As Americans, we proudly hail the work of our scientists. The "information highway" is more than a cliche and is rapidly becoming the thread from which the fabric of our nation is woven. Having been a leader in using automation in my office I can assure you that the law enforcement and legal communities are and, will continue to be, a part of that enterprise. We simply ask that our scientists and engineers put their enormous talents to work in assuring that law enforcement is not left blindfolded. We support a legislative solution that requires the telecommunications industry to meet law enforcement's needs, but that relies upon the industry to decide the most efficient and cost effective approach.

The debate about the need for electronic surveillance in fighting crime has already taken place. The federal government and most state governments have resolved that, in certain cases, and as a last resort, law enforcement may seek an impartial court order to perform limited electronic surveillance. District attorneys support this cautious, restrictive approach. The problems raised by new technologies should not be used as a gambit by opponents of electronic surveillance to reopen this debate. Further, claims by these critics that prosecutors seek increased use of electronic surveillance are simply not true. Let me make it clear that your district attorneys seek nothing more than to preserve the surveillance capability that you, and most state legislatures, have already authorized. We are not asking for help to do any additional wiretaps or pen registers. We are asking only to preserve what Congress and our state legislatures have determined is a critical tool in fighting crime.

This issue is particularly crucial to those of us fighting crime at the local level. Some 60 percent of all authorized criminal wiretap orders are done by state and community law enforcement agencies. Let me hasten to add that the image of a policeman attaching alligator chips to telephone wires to affect a surveillance in as outmoded as the tin-can phones of our youth. Electronic surveillance is a sophisticated, complicated operation not entered into lightly by law enforcement. I would note that in addition to the requirement for a court order based on probable cause, most local jurisdictions have imposed further administrative requirements to preclude abuse of the surveillance. Finally the very industry whose help we seek today serves as a protective balance. I can assure you that local law enforcement does not have the capability to directly intercept telephonic communications and that the telecommunication industry will not provide the requested technical existence in the absence of a court order.

We, as prosecutors can provide many cases to illustrate how critical your support for the Act is and will continue to be. At the local level the ability to conduct electronic surveillance has allowed the successful conviction of drug traffickers who poison our youth, of corrupt public officials to include sitting judges and police officers and RICO cases involving prostitution and money laundering. The issue is often literally life or death. Electronic surveillance is rarely used and is typically used only as a last resort in difficult cases. Judges authorize surveillance only under exacting standards reinforced by rigid and demanding local rules of accountability. But let me assure you that when electronic surveillance is necessary the need is vital.

Criminals who victimize us as a nation have access to and do not hesitate to use, the latest in technology. We, as both citizens and as those who work in the daily fight against crime, urge you not to further handicap our police forces. We strongly encourage the enactment of this comprehensive legislation. Anything short of this approach cannot guarantee our ability to effectively enforce the laws of our nation or our ability to protect our citizens.

Senator LEAHY. Thank you.

Representative EDWARDS. Thank you, Mr. Chairman.

[Whereupon, at 1:25 p.m., the subcommittee was adjourned.]

DIGITAL TELEPHONY AND LAW ENFORCEMENT ACCESS TO ADVANCED TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES

THURSDAY, AUGUST 11, 1994

U.S. SENATE, SUBCOMMITTEE ON TECHNOLOGY AND THE LAW, COMMITTEE ON THE JUDICIARY, JOINTLY WITH THE HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS, COMMITTEE ON THE JUDICIARY,

Washington, DC.

The subcommittees met jointly, pursuant to notice, at 1:10 p.m., in room 2237, Rayburn House Office Building, Hon. Don Edwards, chairman of the Subcommittee on Civil and Constitutional Rights, and Hon. Patrick J. Leahy, chairman of the Subcommittee on Technology and the Law presiding.

Also present: Representatives Coble and Canady, and Senator Pressler.

OPENING STATEMENT OF HON. DON EDWARDS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Representative EDWARDS. The hearing will come to order.

Today, we resume joint hearings with our Senate colleagues. The question before us is how can law enforcement agencies conducting court-authorized wiretaps keep pace with emerging technologies while still respecting privacy and not hampering the innovation that is fundamental to the competitive success of American industries.

Earlier this week, the ranking Republican, Henry Hyde, and I introduced legislation responding to these concerns. Identical legislation was introduced in the Senate by Senator Leahy.

Some have questioned whether there is a need for this legislation at all. I believe that the need is real. The General Accounting Office has looked at the issue and has found that new technologies and services do pose problems for wiretapping.

The FBI has conducted an informal survey of State, local, and Federal agencies and found 183 instances in which technological problems impeded court-authorized wiretaps. The FBI submitted this information to us but asked that it not be publicly disclosed. However, I have received a summary of the information from the FBI and the FBI has agreed it can be released. I will enter it in the record with my statement.

Finally, I believe that the industry itself acknowledges we have a problem, as reflected by the creation of an industry committee to develop solutions for a number of these newer technologies.

We listened very carefully over the last several years to the interest of concerned parties and the bill before us reflects many suggestions from industry and privacy advocates. I must congratulate three of the key participants in this effort.

FBI Director Louis Freeh has been sensitive to the concerns of industry and privacy. While always insisting that law enforcement's basic needs be respected and met, he has recognized that any legislation must be narrowly focused. He has recognized the need for flexibility and a reasonableness standard, and this is going to be reflected in this bill.

Second, I must thank Jerry Berman of the Electronic Frontier Foundation for putting together the dialog that has brought us to this point. Without Jerry, we wouldn't have had a balanced bill that included privacy protections.

Finally, I thank Larry Clinton of the U.S. Telephone Association, who has worked with us diligently. There are many provisions in the bill that reflect the concerns of his members.

I am personally comfortable with the bill. It is a balanced bill. We have gone a long way to accommodate the interests of everybody.

Senator Leahy?

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Thank you very much, Mr. Chairman. I want to commend you for having this hearing and the tremendous work you have done. As I said at the time of the crime bill conference, I am one member of the other body who is going to miss your leadership. Being a colleague of yours has been one of the great joys of my service here in the Senate.

Director Freeh, at our last hearing you identified digital telephony as "the number one law enforcement, public safety, and national security issue facing us today." You and other law enforcement agencies told us difficulties we are going to have as we go into the next century if we can't meet the needs for wiretapping.

I will tell you right at the outset, I do not want law enforcement to lose its capability to use this powerful tool in its crimefighting arsenal. Having spent nearly a decade of my own life in law enforcement, I know how important it is. I know that wiretaps can produce powerful evidence against our most dangerous criminals at the lowest risk to the agents involved. We don't have to make deals with criminals or protect witnesses or expose agents to dangers when the police can convict criminals with taped words out of their own mouths.

But I also want to make sure we don't jeopardize either important privacy rights of all Americans or frustrate the development of new communications technologies. There was a time when the local sheriff could drive up in his pickup truck, stand on the roof, hook alligator clips to the phone, put on the earphones, and know what was being said.

We got concerned there might be a few too many people hooking on the old alligator clips and passed wiretap legislation, which made it very clear that you go through the courts, you do all the things you have to do. So we passed the law that protects people's constitutional rights, but then, the technology changed. We have the law but advancing technology is leaving law enforcement behind in its ability to use that law.

Now you can have a money launderer in Boston calling a drug kingpin in Miami to arrange for a shipment of drugs to come into Los Angeles. Those calls could be going over microwaves or over fiber optic lines. Of course, if it is digitized, it is a bunch of ones and zeroes, and whether you have the alligator clips or something else, you are really not going to find out anything about that money laundering, the drug kingpin, or any part of the criminal conversation. That is not what we want.

We have tried to put together a bill that won't stop technology but will help law enforcement. Congressman Edwards and his staff, my staff, the FBI, telephone companies, and everybody else involved, that have spent hours on crafting a reasonable bill that will assure law enforcement's ability to conduct court-authorized wiretaps.

It sets forth four wiretap capability requirements that telecommunication carriers would be required to meet, so they would know what to do when they set about designing new equipment. Phone companies make sure when they plug in new services that the phone system is not shorted out, so that if I use a new service to call from my farm in Middlesex, VT, to somebody in my office in Washington, DC, we are going to get through. We are not going to short out that system, but we are also not going to short out effective law enforcement.

The privacy and security protections for telephones and computers have been expanded in ways that were first recommended to me by a privacy and technology task force organized back in 1991. The protections in the Electronic Communication Privacy Act of 1986 are extended to cordless phones. We take care of questions about the extent of privacy protection for messages sent over a computer. If you send an E-mail message to somebody, you ought to be protected the same way you would if you picked up the phone. We improve the privacy of mobile phones by expanding criminal penalties for stealing the service from legitimate users. But we do it without impeding innovation in telecommunications services.

Under the bill, law enforcement agencies may not require the specific designs of telecommunications systems or features nor prohibit adoption of such design by any telecommunications providers. Industry, not government officials, will run the show.

I did this because I have always had some frustration with what we have done with telecommunications within the Federal Government. We have studiously tried to stay 15 to 20 years behind the curve. The Department of Defense sometimes at multi-billion-dollar installations will have something that looks like World War II telecommunications. The only thing lacking is somebody turning a handle.

Mr. Neel knows what it was like when the administration went to the White House and found that you have a 1950's system, so poorly designed that when the President asked if he could get a phone of his own they told him, certainly, within a few months they could have one. I suggested that he call the local telephone company and he could probably have it put in that afternoon.

So we don't want that to happen, and we are taking care of many questions. We are still going to have questions remaining about how much it is going to cost and who is going to pay for it.

Mr. Chairman, I will put my whole statement in the record because I suspect that we are going to learn more from the witnesses here than what I would have to say.

[The prepared statement of Senator Leahy follows:]

PREPARED STATEMENT OF SENATOR PATRICK J. LEAHY

At our last joint hearing, FBI Director Freeh identified the digital telephony issue as "the number one law enforcement, public safety, and national security issue facing us today."

The FBI and other law enforcement agencies have told Congress that their ability to conduct wiretaps is being undercut by new communications features and services that are designed with no thought as to how they might affect law enforcement.

I, for one, do not want law enforcement to lose its capability to use this powerful tool in its crime-fighting arsenal. Wiretaps produce powerful evidence against our most dangerous criminals, at the lowest risk to the agents involved. We don't have to make deals with criminals, protect witnesses, or expose agents to danger when police can convict criminals with tapes of their own conversations.

At the same time that I want to assist legitimate law enforcement needs, I want to make sure we do not jeopardize important privacy rights of all Americans or frustrate the development of new communications technologies. I believe the companion bills Chairman Edwards and I introduced on Tuesday achieve those goals.

Over the past few months, I have worked closely with the distinguished Chairman of the House Judiciary Subcommittee on Civil and Constitutional Rights, Don Edwards, to craft a digital telephony bill. I am always delighted to the opportunity to work with the Chairman, whose hard work and deserved reputation for staunchly defending our civil liberties will be sorely missed in Congress upon his retirement at the end of this session.

Our digital telephony bills were carefully hammered out during numerous meetings with House and Senate staff, industry groups, privacy and civil liberties advocates and the FBI. These parties have worked diligently and in good faith in this effort. It has not been an easy task, and we are all continuing to work to resolve this matter.

This bill ensures law enforcement's continued ability to conduct *court-authorized* wiretaps by setting forth four wiretap capability requirements that telecommunications carriers would be required to meet. This means that when the phone companies set about designing and deploying new services or features, they must consider law enforcement's needs among the numerous other factors that go into such designs.

Just as phone companies make sure that when they plug in new services, the phone system is not shorted out so, too, we do not want to short the American people's need for effective law enforcement.

The bill also expands privacy and security protections for our telephone and computer communications in ways that were first recommended to me by a Privacy and Technology Task Force I organized in 1991. The protections of the Electronic Communications Privacy Act of 1986 are extended to cordless phones and certain data communications transmitted by radio.

In addition, this bill increases the protection for consumers when they transact their business over the telephone or send messages over their computers. If you call your bank to transfer money, send E-mail messages to an online discussion group, or order a movie from a payperview service, the bill protects the privacy of your transaction.

The bill further protects privacy by requiring telecommunications systems to protect communications not authorized to be intercepted and by restricting the ability of law enforcement to use pen register devices for tracking purposes or for obtaining transactional information. Finally, the bill improves the privacy of mobile phones by expanding criminal penalties for stealing the service from legitimate users.

The bill does all this without impeding innovation in telecommunications services. Under the bill, law enforcement agencies may not require the specific design of telecommunications systems or features, nor prohibit adoption of any such design, by any telecommunications provider.

The bill protects law enforcement wiretap capabilities, but defers to industry on meeting those needs. Industry, not a government official, runs the show.

To allay public concern over the breadth of wiretapping in America, the entire process remains subject to public scrutiny, oversight and accountability. This bill accomplishes this by requiring any standards or technical requirements that industry adopts to insure wiretap capability be publicly available.

Industry is not hobbled when innovation moves swifter than law enforcement needs. If industry is ready to deploy a new phone feature or service, but lacks current technology to satisfy access for lawful wiretaps, a court can allow the technology to go on line. But if industry can adapt the service to assist law enforcement—it must do so.

Some questions remain that need to be explored at this hearing, including how much is this going to cost and who is going to pay for it. The bill authorizes $500,000,000 toward implementation of any required retrofitting of the system over the next four years. This is based on Director Freeh's previous testimony and the FBI's estimate of costs.

I look forward to hearing from our witnesses about these cost issues and intend to work diligently to resolve this matter this year.

Representative EDWARDS. Thank you, Senator. The gentleman from North Carolina, Mr. Coble?

STATEMENT OF HON. HOWARD COBLE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

Representative COBLE. Thank you, Mr. Chairman.

I don't have a prepared statement but I will say a word or two, Mr. Chairman. You and the distinguished gentleman from Vermont have pretty well echoed my view on this. I share the gentleman from Vermont's concern in that I in no way want to emasculate or weaken law enforcement in its capability, but I am just as concerned and will guard just as jealously the assurance that in hanging onto that capability and even refining it, that we don't trash or scuttle individual rights to privacy.

That has been a very fine line, Mr. Chairman, that we have to pursue in this area of the law and it has always bothered me, the rights of law enforcement on the one hand, which I heartily defend and promote, but on the other hand, I don't care if it is the biggest bum or the biggest crook in town, we cannot trample individual rights to privacy. I am very uneasy about that.

I realize safeguards are in place. Oh, yes, Congress is taking care of that. But I wonder, ladies and gentlemen, how many times that when wiretap authority is granted, how many times that is done as a result of rubber-stamping it as opposed to thorough and deliberate study surrounding the request for the wiretap. That still plagues me. I am not going to give a sermon today, Mr. Chairman, but I wanted to share that with you all and with our panel here today.

Finally, and this is of no small concern either, cost. This is going to cost a whole lot of money. Ladies and gentlemen, in this town, and Mr. Chairman, you know it as well as I do, in this town, bureaucrats have a way of recklessly and indiscreetly flashing out figures. Oh, this is only going to cost $500 million—only $500 million, that is, and then by the time the dust has settled it is going to cost near $1 billion. I am not saying that in this case, but I am saying that happens on this Hill.

So I think we need, Mr. Chairman, to be real adamant in seeing to it that what cost figures are floated are accurately justified and supported and defended.

I thank the chairman and I thank you all for having called this hearing today.

Representative EDWARDS. Thank you, Mr. Coble.

The gentleman from Florida, Mr. Canady?

STATEMENT OF HON. CHARLES T. CANADY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Representative CANADY. Thank you, Mr. Chairman.

I won't repeat the comments that I made at our hearing several months ago. I will just say that based on a preliminary review of H.R. 4922, it appears to me that this is legislation which does strike an appropriate balance and that significant progress has been made in dealing with this important issue. I will look forward to hearing the testimony of the witnesses today. Thank you.

Representative EDWARDS. Thank you.

I think what we will do is introduce each of the witnesses just before they speak, and then after all the statements have been made, we will have a series of questions.

The first member of the panel is Hon. Louis J. Freeh, Director of the Federal Bureau of Investigation. Welcome.

STATEMENT OF HON. LOUIS J. FREEH, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. FREEH. Thank you, and good afternoon to both Chairman Leahy and Chairman Edwards and other distinguished members of the panel as well as your staffs.

It is a great privilege to appear back here today, having discussed this issue in the Committee on March 18, not so long ago, and to really marvel at the remarkable progress that has been made both between the committee staffs and the principals and my colleagues that are sitting here with me this afternoon. I think it is a great testament to the nature of the process and the good faith behind the process that such a critical compromise was reached and such an important result has been obtained.

I have a longer statement for the record, and with your permission, I will just highlight some of the points which I have already made and now which I can make in the framework of this legislative proposal.

We believe that the legislation, as introduced this past Tuesday, offers the strongest investigative assurances that the authority which Congress gave us in 1968 will continue unimpeded by technology. The issue before the Congress and before the public is the updating of the technical assistance requirement embodied in the statute, but of course changed by technology.

I think that a delicate but critical balance has been achieved between public safety and privacy and constitutional rights. If you look at the bill simply and graphically, there are ten provisions. Four provisions are addressed to law enforcement; the other six to privacy. Even within the law enforcement provisions, there are all of the safety valves, both to encourage cooperative design and development but also to prevent by a safe harbor provision the penalties to any member of the community, particularly the common carriers or the equipment suppliers and manufacturers, so if they are unable to achieve a certain agreed-upon standard, either because of technological problems or funding problems, they are protected. That is, by my own admission today, a vast improvement as to the proposal made in the legislation which we discussed earlier this year.

Without question, and I need not repeat this, court-authorized electronic surveillance is a critical law enforcement and public safety tool. I think we have reached a remarkable compromise and achievement in preserving that tool as it has existed since 1968 and yet balancing all the technology and privacy concerns which are so precious to all of us.

The legislation, in our view, is not just a compromise but a victory for all of the interests involved. The legislation reflects reasonableness in every provision: The limited but appropriate scope of coverage, the longer compliance period—4 years as opposed to 3, the specifically-articulated law enforcement capacity requirements, and, as I mentioned, the creation of a safe harbor for industry through the use of technical requirements developed cooperatively between law enforcement and industry standards has now been achieved. All are very reasonable and practical solutions to difficult problems.

Further, the administration proposed and your bills include a mechanism for reimbursing carriers for making modifications necessary to achieve compliance during a more flexible compliance period. In my view, reimbursement is desirable if we are to meet the concerns of industry and still maintain effective law enforcement, ensuring the public safety and protecting national security. I believe the proposed reimbursement should be viewed as a substantial effort to assist industry in meeting the technical assistance requirement imposed by Congress.

We, too, are extremely concerned and appreciative with respect to the estimated costs which would be necessary to fund this proposal. I think with respect to that concern, I would draw very heavily from the excellent GAO report which has been furnished by my colleague to note that the costs, obviously, will be directly related to the solutions.

It seems to me that with the cooperative spirit and the momentum which we have achieved in the discussions of this legislation, the setting of standards and the absolutely priority goal of achieving the most efficient cost-saving methods to achieve them can be attained. Working between the industry and the law enforcement and the standards-setting bureaus, I believe that we can achieve great efficiency and I am hopeful that even the estimated costs, which we have said could vary from $300 to $500 million, could be reduced perhaps with that cooperation with the efficiency and with focusing on the most difficult law enforcement objectives that need to be achieved.

With respect to the security systems involved in these provisions, as pointed out by both chairmen, they do, in fact, enhance privacy and security by requiring, for instance, that switch-based intercept efforts be activated only with the affirmative intervention of a carrier employee, thereby leaving the controls to these systems within the purview and jurisdiction of the telephone companies and not the law enforcement agencies.

Enhanced privacy protection regarding governmental access to stored transactional records is included, which again, by my own admission, is a vast improvement from the initial draft which the Government proposed.

There is the requirement to utilize pen register technology when reasonably available that restricts the recording of electronic impulses to the dialing or signaling information used in call processing. Location information associated with the use of cellular or mobile communications incidental to the execution of pen register court orders is now excluded, another important improvement.

Finally, there are a number of privacy-enhancing amendments to the Electronic Communications Privacy Act of 1986. After numerous meetings and drafting sessions with your excellent and able staffs with the telecommunications representatives, the privacy advocates, a balanced legislative language has been developed. We all recognize that this was and is a difficult issue and one where each of the parties involved approached with not just the wisdom but the spirit of compromise. Public safety demands that the legislative solution be found now.

I would like to take this time to commend you, Chairman Edwards, Chairman Leahy——

Senator LEAHY. You are scaring him away, Director.

Mr. FREEH. That is why I changed the order of it. [Laughter.]

Mr. FREEH. I commend you for the remarkable stewardship, wisdom, and leadership that you have shown, which is appreciated by all the parties represented here at the table.

Just as important, I would like to thank very sincerely your very able staffs, Jim Dempsey and Beryl Howell who are present in the hearing room, Nelson Cunningham and Ken Mendelson who I don't see but who were equally able, competent, extremely patient, and imaginative in solving what I admit was a most difficult problem.

Your efforts will ensure our continued ability to protect lives, property, and the national security. We will also continue in that protection without giving the law enforcement authorities any additional jurisdiction or ability to conduct such investigations and meanwhile balancing those necessary tools against critical privacy and constitutional rights.

We are just delighted and complimentary to you and my colleagues here for what we admit is not only a much better product than we came up with but one which is more likely to do the job. Thank you.

[Mr. Freeh submitted the following:]

PREPARED STATEMENT OF LOUIS J. FREEH ON BEHALF OF THE FEDERAL BUREAU OF INVESTIGATION

Mr. Chairmen, let me thank you for providing me this opportunity to again discuss with you one of the most important issues facing law enforcement today. I also want to express my appreciation at the outset for the commitment and effort that you, your subcommittees, and your staffs have made in assisting law enforcement, and in particular the FBI, in achieving a successful resolution of this very difficult and extremely important issue.

As you recall, on March 18, 1994, I appeared before you and provided a detailed statement fcr the record explaining the tremendous importance of court authorized electronic surveillance to law enforcement, the technological impediments that have been impacting, and will continue to impact, such surveillance, and the dire consequences to effective law enforcement, the public safety, and the national security if no binding solution to this problem is obtained. Further, on March 25, 1994, the administration formally transmitted to the Congress a legislative proposal to address this critical issue. I believe that the legislation that has subsequently evolved, and that was introduced in both houses of Congress this past Tuesday, offers strong assurance that this important investigative technique will be preserved while at the same time also ensuring that the privacy of law abiding telephone users remains fully protected and that the telecommunications industry remains fully competitive, both domestically and internationally.

As I have previously indicated, court authorized electronic surveillance is one of law enforcement's most important and effective investigative techniques and is often the only way to prevent or solve the most serious crimes facing today's society. Because of advances in telecommunications networks, the introduction and deployment of new digitally-based technologies, services and features, law enforcement's ability to conduct court authorized surveillance is being threatened. Industry representatives have acknowledged that existing networks and networks planned for the future prevent common carriers from being able to comply with court orders and provide law enforcement with the needed access to all communications and dialing information set forth in the orders.

Over the past decade, we estimate that several hundred court orders have been frustrated, either in part or in whole, by various technological impediments. A recent informal survey conducted by the FBI, and updated this spring, identified 183 incidence were Federal, State, and/or local law enforcement had been frustrated by such technological impediment and that number is ever increasing.

I believe the legislation before you carefully balances the legitimate concerns of law enforcement, the telecommunications industry, and privacy advocates. It is the product of intense discussion, give and take, and compromise by all parties involved. you, your staffs, the FBI and those representing privacy and industry interests have worked extremely hard, and I believe, been flexible, in order to reach a satisfactory legislative solution which addresses the public safety concerns of the law enforcement community and affords great privacy protection to telephone users. I believe that we have clearly demonstrated that technological impediments to electronic surveillance indeed exist, that Federal legislation is the only realistic solution and, as I indicated on March 18th, that from the outset we have been willing to accommodate every reasonable concern raised by the telecommunications industry and privacy advocates.

Indeed, I believe that a hallmark of your legislation is reasonableness. The language of the legislation reflects reasonableness in every provision. For example, the coverage of the legislation focuses on common carriers—entities that historically have been subject to regulation. We have acknowledged, as have your subcommittees, that almost all of our electronic surveillance problems have occurred, and will continue to occur in the foreseeable future, in the networks and systems of common carriers. therefore, this legislation does not unreasonably and unnecessarily call upon small private branch exchange (PBX) operators, pure computer networks, or private networks to alter their systems and networks. Even within common carrier networks, we have agreed to language which reasonably limits carrier responsibilities in certain key areas. The legislation does not require common carriers to satisfy the electronic surveillance requirements by assuring access to targeted communications where the communications link is one that exclusively is dedicated to interconnecting carriers and private networks. second, information services are excluded. and third, with regard to cellular communications that are handed off to other common carriers or to other service areas, we have agreed to language which specifies that the initial carrier need not artificially reroute communications, and we have settled upon being advised as to identity of the new carrier when such a hand-off occurs.

Because some carriers have expressed a concern about meeting these requirements within three years, as originally proposed by the administration, we have agreed to language which extends this period to four years, and which also permits a carrier to request an extension of up to two more years where the carrier can show that good faith and reasonable efforts require more than the four-year period.

We have also agreed to language which explicitly states that law enforcement may not dictate or require the specific design of features or system configurations, nor may law enforcement prohibit the adoption of any feature or service. As I have said on numerous occasions, law enforcement has no intention of becoming a technology

CZAR or of regulating the development of new and beneficial telecommunications systems, services or features.

Because telecommunications industry representatives have expressed a concern that the administration's proposal did not specifically address the capacities requirements that would be placed on each carrier, we developed, and the legislation includes, provisions which clearly place an affirmative responsibility on the Attorney General to advise carriers of law enforcement's specific capacity requirements within the first year after enactment of the legislation. These provisions will furnish carriers both with our short-term needs and our longer range capacity requirements, such that the required capacity will not be needlessly undersized or oversized.

We have agreed to language regarding carrier reliance upon industry-based technical requirements and standards that meet law enforcement's requirements which serve as a so-called "safe harbor" for carriers and prevent needless concern about civil liability exposure where good faith efforts are made to comply with such technical requirements or standards. Further, in case of any dispute with regard to such technical requirements or standards, any person may petition the FCC to institute proceedings to resolve any conflict and establish appropriate requirements or standards consistent with the electronic surveillance requirements set forth in the legislation.

With regard to enforcement, we have agreed to language that allows a carrier to prevent the issuance of an enforcing court order under circumstances where alternative technologies or technical capabilities exist or where the law enforcement requirements are better met by another carrier. Further, such an order would be precluded where compliance is not reasonably achievable through the application of available technology and timely action has been taken. Finally, an enforcement action is flatly precluded where the capacity demands exceed those for which the carrier has been provided notice. In any case, before a court can assess a civil penalty it would be required to take into account the nature, circumstances, and extent of the violation, and, with respect to the violator, ability to pay, good faith efforts to comply in a timely manner, effect on ability to continue to do business, the degree of culpability or delay in undertaking efforts to comply, and other matters.

Perhaps of greatest concern to the telecommunications industry is the issue of cost. We all recognize this is a highly competitive industry and that the issue of cost had to be addressed to make this solution practical. The administration proposed a mechanism for reimbursing carriers for making the modifications necessary to achieve compliance during the specified compliance period. Your bills do likewise and includes a well thought out dispute resolution process. In my view, reimbursement is desirable if we are to meet the concerns of industry and still maintain effective law enforcement, ensure the public safety, and protect national security. For other public welfare and safety issues, such as the installation of sprinkler systems, smoke detectors, fire alarms, fire escapes, safety belts, and air bags, to name but a few, industry has been required to meet these obligations without the benefit of this type of solution. I believe the proposed reimbursement should be viewed as a substantial effort to assist industry in meeting the "technical assistance" requirement placed on carriers by Congress some twenty-five years ago.

We have also been very willing to address the concerns of privacy advocates, which the provisions of your legislation make clear. First of all, there is the basic requirement that carriers fulfill their electronic surveillance assistance requirements in a manner that protects the privacy and security of communications and information of all subscribers whose communications are not authorized to be intercepted. Second, there are systems security provisions which enhance privacy and security by requiring that all electronic surveillance efforts initiated in switching premises be activated only with the affirmative intervention of a carrier employee. Third, enhanced privacy protection is included with regard to governmental access to any interactive transactions for which a carrier may keep a record. Fourth, law enforcement is required to utilize pen register technology, when reasonably available, that restricts the recording or decoding of electronic or other impulses to the dialing or signaling information utilized in call processing. Fifth, the assistance requirements in these bills exempt the provision of any location information associated with the use of cellular or mobile communications incidental to the execution of pen register court orders. Finally, there are a number of privacy enhancing amendments to the electronic communications privacy act of 1986, the foremost of which is the conferring of privacy protection on the radio portion of cordless telephone communications.

After numerous meetings and drafting sessions with your staff, telecommunications industry representatives, and privacy advocates, balanced legislative language has been developed that, I believe, is acceptable to the affected parties. We all recognize that this issue is a difficult one, one which each of the parties approaches from a distinctly different vantage point. All parties have work hard and all have been flexible. it is understandable that a small number may not be enthusiastic or strong advocates for legislation. However, public safety demands that a legislative solution be found and found quickly. I believe that this is why everyone made concessions and reached acceptable compromises. I also believe that this is why all acknowledge that your legislation is reasonable and acceptable as a means of resolving this critical law enforcement problem in light of the competing concerns and considerations.

Once again, I would like to personally thank both Chairman Edwards and Chairman Leahy, the members of the Subcommittees and your staffs, in particular Jim Dempsey, Beryl Howell, Nelson Cunningham and Ken Mendelson, for taking on this difficult issue and for your unwavering support for the enactment of legislation to resolve this problem during this session of Congress. This is a "drop dead" issue for law enforcement. Your efforts will ensure law enforcement's continued ability to protect the American public and safeguard our national security through the use of this vital investigative technique, while being ever mindful of legitimate privacy and industry concerns. At this time I would welcome any questions you may have.

DIGITAL PRIVACY AND SECURITY WORKING GROUP,
Washington, DC, March 11, 1994.

Mr. LOUIS J. FREEH,
Director, Federal Bureau of Investigation,
Washington, DC.

DEAR DIRECTOR FREEH: This letter is a follow-up to our letter of March 9, 1994 to President Clinton and Vice President Gore (a copy is attached). While we do not believe that new legislation is needed to accomplish the FBI's goals, we take this opportunity to more specifically raise some of the questions that should be answered in pursuing any digital telephony legislation. The draft that the White House has given us for comment is overly broad, and it is our hope that this letter will assist in narrowing the scope of any legislation.

While we have additional, important questions and concerns, this letter sets forth our primary concerns.

(1) Should digital telephony legislation reach "call setup information" independently of a "Title III" search warrant?

The New York Times of February 28, 1994 quotes you as stating, "My real objective is to get access to the content of telephone calls." The bill should therefore be limited to content of communications and incidental call setup or transactional data.

Legislation should apply to "call setup information" only when that information is incident to a warrant issued for wire, oral, or electronic communications as set forth in 18 U.S.C. §2518. Extending the legislation's scope beyond the acquisition of content (pursuant to a warrant under section 2518) to the independent acquisition of call setup information raises many issues that require examination. For example, currently the legal standard for obtaining transactional data is a certification (via subpoena or statement to a judge) that the sought-after data is relevant to an ongoing criminal investigation. In the era of personal communications services ("PCS") and of the information highway, transactional data will reveal far more about individuals than it has in the past. In fact, in some cases it may be equivalent to content information. Thins transactional data certainly could make it possible to build a detailed model of an individual's behavior and movements. The net result could be government dictating to industry that it create a surveillance-based system that will allow federal, state, and local government to use a service provider's electronic communication facilities to conduct minute-by-minute surveillance of individuals.

As long as they have an IRS or other administrative subpoena or a law enforcement agent willing to certify that the sought-after data is relevant to an ongoing criminal investigation law enforcement officials could demand that they be notified at some remote location every time certain individuals communicate by telephone and their location at the time, as well as every database they connect to and when they log on and off. In short, law enforcement officials could insist on instantaneously knowing the existence of every single electronic communication (but not its content).

The enormous potential for abuse and threat to personal privacy suggests that, if transactional data were to be covered by digital telephony legislation, it should be incidental to a "Title III" wiretap warrant. This would not limit in any way law enforcement's access to trap and trace, pen register, or call billing information under current law or practice. This is particularly true given that there has been no case made that demonstrates any current or potential difficulty in getting this noncontent information under current practices. The technology in fact has made these type of services much easier for law enforcement to use and access. Additional legislation is simply not necessary to obtain this data.

(2) What is covered?

The obligation to isolate the content of communications must be reasonably related to the service provider's telecommunications services. It would be unreasonable for the FBI to demand any person involved with the communication to furnish it with access to that communication. For example, most providers, including local telephone companies, usually need to isolate communications for purposes of billing and maintenance. It is appropriate for the FBI to seek their assistance in intercepting communications on their networks only when the requests are reasonably related to the telecommunications services they provide.

Therefore, the question is not necessarily who is covered, but what telecommunications services are covered. For example, the legislation should reflect the fact that, in reselling services, even local telephone companies sometimes are unable in those instances to furnish call setup information regardless of whether it is incident to the acquisition of a communication's content.

(3) What will be the requirements placed upon service providers and what will be the standard of compliance that will be applied?

Legislation should carefully define the obligations of service providers. This is not the case with the FBI's current draft of proposed legislation. These obligations are vague and subject to considerable interpretation. Service providers and manufactures must have flexibility to adopt procedures that reasonably comply with the specific functional performance requirements of law enforcement.

This is particularly true where, as here, compliance requires an assessment of future needs and interoperability requirements. There is a difference between compliance and a guarantee, and legislation must reflect that difference. Carriers should be required to provide reasonable cooperation and that cooperation should be measured by a standard of reasonable compliance.

In installing new software or equipment under this statute, a service provider must be able to reasonably assess future demands by law enforcement. Other industries subject to regulation at least know, for example, the temperature at which they must maintain the specimens, the emission standard they must satisfy, or the type of safety restraint equipment they must install and the date by which they must have it installed in vehicles. Service providers cannot be held to an absolute standard of compliance where they are using and delivering new technologies to the public and the demands of law enforcement are not clearly specified. This applies to both capability and capacity. Law enforcement must be specific in its requirements for capacity and capability from each service provider.

(4) What is expected of commercial mobile service providers?

It is not a foregone conclusion that mobility in a digitized telecommunications environment will degrade or otherwise impede the law enforcement community's ability to effectively execute court-approved wiretap orders.

Wireless carriers are committed to assisting law enforcement agencies to successfully wiretap and intercept voice communications. To accomplish this goal, the wireless industry understands that available excess port capacity is needed in all switches throughout the nation. While it may be reasonable for federal and state law enforcement agencies to acquire the contents of wireless communications pursuant to "Title III" warrants through additional port capacity, it would be prohibitively expensive to require that every one of the nation's switches be connected to the FBI to enable it to acquire such information on a "real time" basis at remote locations.

Connecting every one of the nation's switches to the FBI, moreover, would increase exponentially the risk of unauthorized access to wireless communications. Further, the proliferation of fraudulent use of wireless telephones through such techniques as "cloning" and "tumbling" ESN's (electronic serial numbers) poses additional questions with respect to privacy and the ability of law enforcement to properly execute court-approved wiretap orders.

(5) What are the responsibilities of manufacturers and suppliers, if any?

The FBI wishes manufacturers of telecommunications equipment and providers of support services to fall within the scope of the legislation. But, would service providers be held liable for software or hardware that is not available from vendors? Why? How would the obligations be enforced against foreign manufacturers? What would be the liability of a domestic carrier that relies upon foreign manufacturers? What are the trade implications of having domestic manufacturers export equipment designed for governmental surveillance?

(6) How, and during what period, are costs to be recovered to ensure that there is a direct relationship been the costs reasonably incurred by covered entities and the government's requirements?

Government should pay for what it needs, which will help focus attention upon the facilities that truly need upgrading. if the government does not pay for upgrades or facilities, then the service providers should not be held responsible. The FBI appears to have accepted the concept that government should pay for the costs of compliance but has so far underestimated these costs and proposed an arbitrary three-year limit on cost reimbursement. Government compensation should be ongoing with industry's compliance.

We trust you find our comments helpful. We remain prepared to work with you, Congress, and others to attempt to resolve the legitimate concerns of law enforcement.

Sincerely yours,

JERRY BERMAN,
RONALD PLESSER.

DIGITAL PRIVACY AND SECURITY WORKING GROUP,
Washington, DC, March 9, 1994.

President William J. Clinton,
The White House, Washington, DC.

Vice President of the United States,
U.S. Senate, Washington, DC.

DEAR MR. PRESIDENT AND MR. VICE PRESIDENT: Telecommunications carriers and other members of the Digital Privacy and Security Working Group are keenly aware of the concerns raised by the Administration regarding the ability to intercept communications transmitted over advanced communications networks.

We are concerned, however, about the nature of the process upon which the Administration has embarked to address these issues. Seeking immediate industry reaction to the FBI's draft legislation and congressional passage of such legislation shortly thereafter is troubling. It suggests curtailment of public debate and of congressional deliberation. Given the interest of the public in these matters and their complexity, it is essential that there be a full public debate on these issues.

Industry is currently cooperating with appropriate authorities to avoid fixture problems and to expand existing capacities. This is not to say that there have not been some transitional concerns particularly upon the introduction of new technologies that have grown greatly in popularity. But, whenever transitional problems have arisen, industry representatives have worked with law enforcement officials to resolve them.

The FBI's actions are especially troubling in light of our view that legislation is not needed to accomplish the Agency's goals. We still see no evidence that current law enforcement efforts are being jeopardized by new technologies. Nor are we convinced that future law enforcement activities will be jeopardized given industry cooperation.

We still believe that continued cooperation by government and industry within the working relationship that has emerged from the 1992 Quantico Joint Government Industry Group will resolve "the digital telephony problem" and preserve the government's current authorities. The discussions have succeeded in identifying specific problems and have begun the process of generating concrete, cost-effective solutions. This process has facilitated a more robust exchange of technical information and an identification of possible new equipment and police tactics needed to achieve law enforcement goals. Nevertheless, we are prepared to work with the Congress and the Administration to attempt to resolve the legitimate concerns of law enforcement.

The signatories to this letter cannot overemphasize how critical it is that any new initiatives in this area preserve the public's confidence in the privacy of information carried over the public switched network. Less than a decade after enactment of the Electronic Communications Privacy Act of 1986, the nation can ill afford to undercut customer privacy expectations. Indeed, on the eve of the National Information Infrastructure's deployment, preserving customer confidence is all the more important. Privacy protection is not a secondary interest here. Survey after survey performed by Professor Alan Westin and others have demonstrated the public's concern with privacy and the security of their communications. We all must seek to maximize those interests and assure the public that their communications are protected.

Sincerely yours,

APPLE COMPUTER, INC.,
AT&T,
AMERICAN CIVIL LIBERTIES UNION,
BUSINESS SOFTWARE ALLIANCE,
CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION,
COMPUTER BUSINESS EQUIPMENT & MANUFACTURERS ASSN.,
DIGITAL EQUIPMENT CORPORATION,
ELECTRONIC FRONTIER FOUNDATION,
ELECTRONIC MESSAGING ASSOCIATION,
GTE CORPORATION,
INFORMATION INDUSTRY ASSOCIATION,
INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA,
IRIS ASSOCIATES, INC.,
MCCAW CELLULAR,
MCI COMMUNICATIONS CORPORATION,
PEOPLE FOR THE AMERICAN WAY,
SOFTWARE PUBLISHERS ASSOCIATION,
SUN MICROSYSTEMS FEDERAL, INC.,
TRUSTED INFORMATION SYSTEMS,
UNITED STATES TELEPHONE ASSOCIATION.

CONGRESS OF THE UNITED STATES,
Washington, DC, April 11, 1994.

Hon. LOUIS J. FREEH,
Federal Bureau of Investigation,
J. Edgar Hoover Building, Washington, DC.

DEAR DIRECTOR FREEH: The Subcommittees are eager to continue their hearings on digital telephony, and would like to ask for your assistance in expediting our consideration of this issue.

A critical point of controversy at our last hearing was whether there are current or prospective impediments that cannot be resolved by industry/law enforcement cooperation. You testified that an informal FBI survey of federal, state, and local law enforcement agencies had disclosed 91 instances of technological impediments to law enforcement surveillance.

The telephone industry testified, as they have indicated on other occasions, that they were unaware of any problems that have not been solved, or are on the way to being solved, through cooperation.

Before we proceed with our next hearing, we request the details of the 91 instances (and any others that you can identify) so we can provide them to industry witnesses and get their response at the hearing. The exact number of instances is not important; what is important is being able to identify specific cases, so industry and law enforcement witnesses can discuss how legislation would deal with those cases in a way that the voluntary efforts have not.

For this purpose, we are requesting copies of the responses to your informal survey. You may, of course, redact any names of subjects and local case numbers. We only need to know the date, the law enforcement agency, the service provider, the type of service, the type of impediment, and any steps taken to resolve the problem. We would like to receive this information as soon as possible so that all witnesses would have an opportunity to respond to it in an informed fashion.

As our staffs have already discussed, we believe that this information is necessary to complete the record of the hearings. We look forward to your prompt response.

Sincerely,

DON EDWARDS,
Chairman,
Subcommittee on Civil and Constitutional Rights.
PATRICK J. LEAHY,
Chairman,
Subcommittee on Technology and the Law.

TECHNOLOGY-BASED PROBLEMS ENCOUNTERED BY FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT AGENCIES

Total Problems	183
Cellular port capacity	54
Inability to capture dialed digits contemporaneous with audio	33
Cellular provider could not intercept long-distance calls (or provide call setup information) to or from a targeted phone.	4
Speed dialing/voice dialing/ call waiting	20
Call forwarding	10
Direct Inward Dial Trunk Group (The provider was unable to isolate target's communications or provide call set-up information to the exclusion of all other customers)	4
Voice Mail (provider unable to provide access to the subject's audio when forwarded to voice mail or retrieve messages)	12
Digital Centrex (provider unable to isolate all communications associated with the target to the exclusion of all others)	4
Other*	42

This information was collected through informal survey of Federal, state, and local law enforcement agencies who voluntarily participated.

*Other problems include:

- Inability of the provider to provide trap & trace information.
- Inability of the provider to isolate the digital transmissions associated with a target to the exclusion of all other communications.
- Other calling features such as Call Back, etc.
- Inability of the provider to comprehensively intercept communications and provide call set-up information.

GTE CORPORATION,
Washington, DC, April 5, 1994.

Congressman DON EDWARDS,
Chairman, Civil and Constitutional Rights Subcommittee,
U.S. House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: I am writing to clarify the record regarding statements attributed to me by FBI Director Freeh during his testimony before the Joint Judiciary Subcommittee hearing March 18 on digital privacy.

Director Freeh referenced comments made by a GTE representative during a recent FBI briefing regarding the proposed wiretap legislation I did participate on behalf of GTE at the above-mentioned meeting and discussed the telephone industry's need to better understand the FBI's technical requirements for the inception of transmissions over advanced communications networks. However, I do not agree with Director Freeh's apparent interpretation of my comments to indicate that GTE was supporting a legislative solution. Rather, my intent was to move beyond the policy debate to a discussion of the technical issues and how best to solve them.

I hope this clarification proves helpful. GTE looks forward to working closely with both the Congress and the Administration in the examination of this important privacy issue.

Please do not hesitate to contact me if I can be of further assistance.

Sincerely,

SAMUEL F. SHAWHAN,
Vice President,
Government Affairs.

U.S. DEPARTMENT OF JUSTICE,
FEDERAL BUREAU OF INVESTIGATION,
Washington, DC, April 7, 1994.

Hon. DON EDWARDS,
House of Representatives,
Washington, DC.

DEAR CONGRESSMAN EDWARDS: Director Freeh appreciates the time you took to discuss digital telephony. As you know, this is a vital issue to law enforcement agencies as well as the American public as we attempt to combat violent crime in this country.

On March 25, the Administration transmitted digital telephony legislation to Capitol Hill. I have enclosed a copy of this proposed legislation in addition to letters sent from the Department of Justice to Vice President Gore and Speaker Foley. I have also taken this opportunity to enclose materials in question/answer format which address issues that have been raised.

If you have any questions or concerns, please do not hesitate to contact me personally. I look forward to your support of this critical legislation.

Sincerely,

JOHN E. COLLINGWOOD,
Inspector,
Office of Public and Congressional Affairs.

LOUIS J. FREEH'S RESPONSES TO QUESTIONS SUBMITTED BY CONGRESSMAN EDWARDS

Question 1. The telecommunications industry has indicated a willingness to work with law enforcement on the digital issue. Additionally nothing has been presented to the Committee that development efforts by industry should be modified/altered at this time. If in fact, a problem exists, what does the FBI perceive the current problem to be and please comment on the urgency associated with the problem.

Answer. Industry Representatives, in fact, acknowledge that existing networks offering these services and features, as well as networks planned for the future, in their current and planned configurations, often prevent, and will continue to prevent, common carriers from satisfying court orders and providing the needed access to all communications and dialing information. Support continued dialog between industry and law enforcement. However, the working group process and the standards body forum now being used is *voluntary* and alone is not equipped or chartered to solve the problem or ensure implementation of solutions. Industry also recognizes this major shortcoming. There is no mechanism, no resolution, short of legislation that can compel a timely, comprehensive, and binding solution.

Question 2. The digital telephony issue is described as the most important and crucial issue facing law enforcement today. However, statistics provided to the Committee indicate that the FBI's share of court ordered criminal wiretaps amount to only .06 percent. Why then, is this issue so critical at this time?

Answer. Contrary to statistics provided by the Committee, the FBI's share of Title III criminal intercept orders in 1992 amounted to 74 percent of all Federal authorizations and 27 percent of the total law enforcement authorizations. Even though these percentages are significant, the proposed legislation is not designed solely to benefit the FBI, but will provide continued court ordered access to assist all of law enforcement in meeting their investigative responsibilities.

Question 3. Will the courts or law enforcement agencies be required to change their review and approval procedures and as a result allow law enforcement to do more than they do now?

Answer. No change in review procedures will occur. Applications to a District Court Judge or the Foreign Intelligence Surveillance Court will still undergo thorough internal review to ensure they comply with standards and requirements. Surveillance applications will be presented by affidavit for review and accompanied by a court order to be signed.

Question 4. Electronic surveillances last for limited periods and are then reviewed for renewal. At the conclusion of a surveillance, individuals are notified that they have been tapped. They then have the opportunity to attack the wiretap. Are these proceedings being made inadequate by this proposal?

Answer. Criminal electronic surveillances last for a set period. At the end of this period they are reviewed or discontinued. Individuals surveilled are then notified of the court order. In a pretrial hearing, surveillance orders cab be attacked based upon the probable cause stated in the affidavit. At trial the court order can also be attacked. These means of attacking an electronic surveillance will not be changed by the current proposal.

Question 5. There are currently a number of persons who are incarcerated based upon their convictions through evidence gathered by telephonic surveillance. Similarly, there are former hostages alive today because electronic surveillances produced information that led directly to their rescues. Do you believe that the loss of this kind of information is outweighed by a potential gain in privacy or financial savings? Can we jeopardize this valuable source of information?

Answer. The productiveness of telephonic surveillances in the drug war can not be overstated. Drug conspiracies are difficult or impossible to penetrate. The introduction of undercover Agents is often impossible because they do not share the same national origin and are not accepted as outsiders. Equity difficult is developing informants within the inner circle of such groups. Virtually all major drug cases, over the past years, have employed some form of telephonic surveillance. The information produced by these wiretaps often is enough in and of itself to produce convictions.

Question 6. Crime is at the forefront of the Administration's and the public's concerns. We are expending billions each year to address criminal problems. How will enactment of the Government's proposal further our efforts to address crime?

Answer. The legislation will preserve the viability of an effective electronic surveillance capability. This technique is critical to fighting our worst and most dangerous crime problems—drug trafficking, terrorism, and violent and organized crime.

Question 7. Could you refresh our memory on the standards of approval for: Criminal electronic surveillances; Foreign Intelligence Surveillance Act (FISA) surveillances; Court order; Grand jury subpoena.

Answer. FBI criminal intercepts must first be approved by FBI Headquarters and then by certain designated officials at the Department of Justice. Criminal telephone surveillances may only be used to surveil persons believed of committing a list of criminal violations. Certain state officials are authorized by Federal law to apply for court orders from state court judges if the particular state has enacted an electronic surveillance statute. Applications must include a writing under oath containing: The name of the law enforcement officer applying for the order; A full statement of facts to justify the order that a particular crime is being committed; A description of the location or facilities from where the communication is to be intercepted and the type of communication to be intercepted; Statement that other investigative procedures have been tried and failed or appear unlikely to succeed or would be too dangerous; Statement of the duration requested; Statement regarding previous applications; and if request is for an extension—states the results to date. The Judge may require other information. Judge must find there is probable cause the individual is committing, has committed, or is about to commit a particular offense. The order may require periodic progress reports. There is an emergency procedure which requires the submission of an approval order within 48 hours. FISA orders require a comparable submission as detailed above for criminal interceptions but the standard is not probable cause that a crime has occurred but is specific and articulable facts that give reason to believe that national security has been or will be jeopardized. Reason to believe the information sought is relevant to a criminal investigation determined by a neutral and detached magistrate. Relevancy to a criminal investigation.

Question 8. Director Freeh, how much does the Government intend to pay for telephone system retrofit? How will this be funded after the initial $500 million is exhausted? What will this cost if not implemented soon?

Answer. $500 million. First of all, it is not at all clear that the costs will exceed $500 million. If there are costs that exceed this amount, we would have to seek additional authorization and appropriation of funding. To delay the implementation will either mean it will be done at a much higher cost later and effective law enforcement will be much more harmed and the public safety put at greater risk.

Question 9. Will the courts or law enforcement agencies be required to change their review and approval procedures and as a result allow law enforcement to do more than they do now?

Answer. No change in review procedures will occur. Applications to a District Court Judge or the Foreign Intelligence Surveillance Court will still undergo thorough internal review to ensure they comply with standards and requirements. Surveillance applications will be presented by affidavit for review and accompanied by a court order to be signed.

Question 10. Do you contend that individuals should be given a higher level of privacy as a result of advances in telephone technology? Exactly what is the Government asking for from the communications industry?

Answer. We continue to support the need for individuals to be secure in their communications. However, we must also recognize law enforcement's responsibility to be able to intercept communications of criminals using the telecommunications systems to further their illicit activities. The Government requirements are: Expeditiously provide law enforcement access to the communications and call setup information of the subjects named in the intercept authorization. Execute all court orders and lawful authorizations for electronic surveillance, including authorizations for multiple, simultaneous intercepts. Provide the ability to intercept the content of communications and acquire call setup information concurrent with the communications of the subscriber who is named in the authorization, to the exclusion of any communications of call setup information of any other subscriber. Provide access to communications content and call setup information regardless of the mobility nature of the facility or service that is the subject of the court order or the use by the subject of any service features. Allow unobtrusive access to the communications content and call setup information with a minimum of interference with any subscriber's service. Transmit the intercepted content of communications and call setup information in a generally available format to a location identified by the law enforcement agency for monitoring purposes.

Question 11. What is the penalty for conducting an unauthorized electronic surveillance? Will the enactment of the proposal impact current prohibitions?

Answer. There are a number of penalties. Generally, the penalty is: (1) Imprisonment up to five (5) years and/or (2) Civil damages, the *greater* of actual damages; $100/day for each day of violation, or; $10,000.

Punitive damages also may be available. There are lesser penalties for certain first time offenders regarding cellular telephone interceptions.

No, the proposed legislation *explicitly* states there is no alteration in the current penalty provisions.

Question 12. Could you explain the problem with "Digital Telephony?"

Answer. Traditionally, common carriers have offered essentially "fixed point" telecommunications: that is to say, communications generated by, or intended for, a customer and transmitted to a fixed location corresponding to a specific telephone number. In the past, when law enforcement agencies conducted court-authorized electronic surveillance or "wiretaps" on a subject the telephone companies were able to provide law enforcement with a location or access point that would virtually assure the interception of all communications associated with the subject's telephone number set forth in the court order.

Recent and continuing advances in the telecommunications industry has resulted in technologies and services (such as cellular communications, call forwarding, etc.) that negate the necessity for communications to be transmitted to a fixed point. In fact, emerging technologies will enable users to initiate and receive calls without regard to their geographical location. Additionally, technologies that allow for the efficient transmission of multiple simultaneous communications of many subscribers over fiber optics and other wire facilities are baking it increasingly difficult to isolate the communications specific to the telephone number in the court order to the exclusion of all the other subscribers' communications.

Question 13. How many court orders for telephonic surveillances were obtained in Fiscal year 1992? Total law enforcement—non FISA; Federal law enforcement—non FISA; State and local law enforcement; FBI—non FISA; FISA; Pen register orders.

Answer. For fiscal year 92–91—9 criminal telephonic surveillance orders for all law enforcement; 340 Federal law enforcement criminal orders; 579 state and local criminal orders; 252 FBI criminal orders; 484 total FISA orders; Estimated at approximately 9,000 pen register orders.

Question 14. In your statement you made reference to a survey that was done by the FBI in 1993 to collect information on technology based problems encountered during electronic surveillance. Could you please elaborate?

Answer. During contacts with other Federal, state and local law enforcement in 1993, the FBI informally asked for instances in which electronic surveillance was frustrated in whole or in part by technology. As a result of this query we received 91 responses from agencies that were willing to share this information. The results are as follows: 30 Cellular—inability to intercept in whole or in part, call content and/or dialed number information; 10 Cellular—inability to initiate intercept due to insufficient switch or port capacity. 29 Custom calling features—call forwarding, abbreviated dialing features; 15 Digital voice lines, fiber optic lines; 4 other custom calling features; 3 Other technology issues.

NOTE: These results do not include situations where court orders were not sought due to technical impediments known in the past to preclude effective execution of the court order. (i.e. cellular capacity.)

Examples:

1. A Federal investigation of a major narcotics organization operation in the northeastern U.S. was hampered when the cellular telephone service provider was unable to fulfill requests for court-ordered wiretaps due to the provider's technical limitations.
2. An organized crime and drug trafficking task force investigation in the southeastern U.S. was unable to conduct a court-ordered wiretap as the cellular service provider as unable to provide lab enforcement with access to the subject's long distance communications made through the provider's cellular service.
3. Two different cellular service providers in the mid-western U.S. were unable to comply with separate Federal court-orders requesting pen register or dialed number information from suspected drug traffickers' cellular telephones.
4. A regional telephone company in the mid-western U.S. was unable to provide a Federal law enforcement agency with the content of dialed number information from a suspected drug trafficker's telephone as a result of the subject's use of custom calling features offered by the telephone company.
5. A cellular service provider in the south was unable to comply with a Federal court-order for dialed number information concerning a Federal public corruption investigation due to the provider's technical limitation.

Question 15. We understand that advanced telephony will create much more information regarding a customer's calling practices, etc. This information is used for billing purposes and is called transactional data. Will the proposed bill permit access to this transactional information? Will you get it by Grand Jury Subpoena? Do you plan to access this information?

Answer. It is not the FBI's intention to get any information regarding content of the message of the telephone call beyond that information that describes the call itself without a court-authorized surveillance order. Data not related to substantive call content may be valuable in certain situations and will be sought when advantageous. Call billing or stored information will be obtained by Grand Jury Subpoena any information regarding the content of the call—or that was not stored by the telephone company will be obtained by Title III order. Non substantive content will be obtained by Grand Jury subpoena. We will seek any information that may further a criminal investigation.

Question 16. Is there any way to assess the endangerment to public safety and national security if this proposal is not enacted?

Answer. I can assure you that a loss or diminishment of such surveillance will produce the following disastrous results: An increased loss of life, attributable to law enforcement's inability to prevent terrorist acts and murders. An increase in corruption and economic harm to business, industry, labor unions, and society generally, amounting to billions of dollars, caused by the growth of undetected and unprosecuted organized crime, public corruption, and governmental fraud. An increased availability of much cheaper narcotics and illegal drugs—along with the personal, societal, and economic harm brought about by increased drug use: that is, the numerous deaths, ravaged lives, increased health care costs, and the tremendous economic harm calculated in the billions of dollars. A substantial increase in undetected and unprosecuted violent crime (bombings, murders, and other violent acts) along with the loss of hundreds of lives and millions of dollars in economic harm.

Question 17. It has been represented to the Committee that FBI field Agents have experienced difficulty when working with telecommunications service providers in implementing court ordered wiretaps. However, following a FOIA request filed by the Computer Professionals for Social Responsibility (CPSR), no such difficulty was indicated. Realistically, *is* there in fact a problem in this regard so as to warrant the proposal of this legislation by the Administration?

Answer. Pursuant to a recent FOIA request by the Computer Professionals for Social Responsibility (CPSR), the FBI released information indicating that, during a specific time frame, a few FBI offices were not experiencing wiretap intercept problems caused by advanced technologies. CPRS has publicly stated that this information indicates there is NO present technological impediments to wiretaps. This assertion is false and misleading. The FBI did not release "positive information" which indicated specific problems. This "positive information" was not released because it either identified ongoing investigations or specifically identified vulnerabilities in electronic surveillance associated with Criminal or National Security Investigations.

During a 1993 informal survey targeting technical problems encountered by law enforcement in conducting court-ordered wiretaps, 91 instances were identified as incidents in which law enforcement was precluded, either partially or fully, from implementing the court order. In fact, in 1992, one state law enforcement agency advised the FBI that approximately 25 percent of its electronic surveillances were impeded by advanced telecommunications technology.

Question 18. The Committee believes that the legislation proposed by the administration will restrict the future development of digital telecommunications and possibly diminish economic competitiveness in terms of the world market. Please comment.

Answer. The legislation proposed *will not* restrict the future development of digital telephony. As a practical matter, it will have no impact on technological development at all. The purpose of the Administration's legislation is to preserve law enforcement access to court-authorized electronic surveillance and in no way affects future advances in technology.

Regarding economic competitiveness, other Governments throughout the world look to the United States as the world leader in telecommunications technology and development. Equally important, foreign governments also are interested in the ability of both government and law enforcement to gain lawful access to developing telecommunication systems for law enforcement purposes. In conferences held with other countries on this issue, these nations indicate they are following this issue in the United States with great interest as they seek to remedy this problem in their country.

Question 19. Can you describe how the current proposal will reduce the privacy of individuals?

Answer. The privacy of individuals will not be reduced. Digital telephony will enhance privacy by making it more difficult for any possible unauthorized wiretaps to occur. The standard for judicial authorization will not be changed. Law enforcement expects that there will be virtually no change in the numbers of intercepts performed annually.

Senator LEAHY. Chairman Edwards has just stepped out for a vote, as have our other colleagues from the House, but we will continue on with the hearing. I suspect the two of us will also have to vote from time to time.

Ms. Hazel Edwards is the Director of Information Resources Management and General Government from the General Accounting Office. Ms. Edwards, your testimony is very interesting in the questions it raises. Please go ahead, ma'am.

STATEMENT OF HAZEL EDWARDS, DIRECTOR, INFORMATION RESOURCES MANAGEMENT/GENERAL GOVERNMENT, GENERAL ACCOUNTING OFFICE

Ms. EDWARDS. Thank you. Chairman Leahy, members of the committees, it is my pleasure to be here to discuss the proposed legislation. My comments will address three aspects of wiretapping, specifically the challenges facing law enforcement agencies. The second area of focus will be on the status of efforts to resolve those challenges. The third area of focus will be on cost.

In July 1992, we reported to Congress that law enforcement's ability to execute court-approved wiretaps was challenged by advanced telecommunications technologies. To update our understanding of the changes that have occurred over the intervening years, we discussed the full range of these technologies and special features with industry and with law enforcement communities. We found that although some technical solutions have been developed to enable wiretaps, further advances in the technologies have made the overall task of intercepting calls more difficult.

As a practical matter, some law enforcement agencies reported that they have encountered problems in affecting wiretaps. In some cases, investigations were delayed or court orders were simply discarded because of these problems. Industry representatives confirm that there are current as well as imminent technologies that are difficult to wiretap.

As a result, Mr. Chairman, we believe that an important tool for law enforcement's investigations is slowly vanishing. Clearly, there is a need for action that will preserve law enforcement's ability to conduct court-approved wiretaps.

Regarding the status of efforts to resolve these challenges, we reported in 1992 that law enforcement agencies had not sufficiently defined the requirements for wiretaps. That is now changing. Law enforcement agencies have made progress in describing their needs in terms of both capability and capacity.

As of June of this year, the capability requirements are clearly stated. However, the technical solutions for delivering these capabilities have not yet been defined by the service providers and manufacturers. Capacity requirements are not yet defined. Capacity needs would include detail on, for example, the number of simultaneous wiretaps that would need to occur as well as the identification of specific locations where wiretap capability would be needed.

In June of this year, the requirements document acknowledged that both law enforcement agencies as well as industry must collectively determine the level of capacity needed to implement wiretaps.

Now to the issue of cost. The proposed legislation authorizes the Attorney General to reimburse telecommunications carriers for reasonable costs incurred in carrying out provisions of this bill. The bill also authorizes the appropriation of $500 million for this purpose during the years 1995 through 1998.

It is virtually impossible to precisely determine if $500 million is adequate to cover the reimbursement costs of the provisions discussed in this bill because cost will depend on the evolving capacity requirements as well as on the yet-to-be-determined technical solutions.

For example, if law enforcement requires capacity beyond what is available in current switch technology, then switch upgrades will be needed to attain desired capacity levels. The cost of these upgrades could vary considerably, depending on the number of switches involved. In the case of land-line switches, there are more than 20,000 switches nationwide.

To further illustrate the difficulty of precisely estimating the cost associated with this bill, consider the following scenario. Industry cost estimates for land-line switch upgrades range from somewhere in the neighborhood of $15,000 to upwards of $100,000 per switch, depending, of course, on the extent of changes required in the hardware and software.

Assuming that law enforcement will require nationwide access to wiretapping capability for land-line services, then the cost of upgrading all 20,000 switches would range from the hundreds of millions of dollars into the billions of dollars.

I will conclude my remarks with three observations that could help control the cost of this initiative. The first is that as technical solutions are developed, law enforcement and industry should find effective ways to share the solutions and thereby avoid unnecessary cost.

Second, law enforcement and industry should prioritize the development of solutions to address the most critical needs first and where possible control costs by coordinating switch upgrades to coincide with the upgrades already planned by the service provider.

Finally, law enforcement agencies and industry should make wiretap requirements part of the industry's standards which guide the design and the development of new and emerging technologies. Incorporating these needs at the beginning of the product cycle should help lower the overall and ultimate cost of meeting law enforcement's needs.

Mr. Chairman, that concludes my remarks. I would be happy to respond to any questions from you or other members of the committees.

[The prepared statement of Ms. Edwards follows:]

Prepared Statement of Hazel E. Edwards, Director, Information Resources Management/General Government Issues, Accounting and Information Management Division

Mr. Chairman and Members of the Subcommittees: I am pleased to appear today to discuss S. 2375. My comments will focus on the wiretapping challenges facing law enforcement agencies, the status of law enforcement's technological requirements, and the potential costs of satisfying those requirements.

TRADITIONAL WIRETAPPING METHODS ARE CHALLENGED BY TECHNOLOGY

In July 1992, we reported to the Congress that law enforcement's ability to execute court-approved wiretaps was challenged by advanced telecommunications technologies.[1] To determine the current status of digital telephony and to identify the changes that have occurred during the last 2 years, we interviewed representatives from law enforcement organizations, telephone service providers, and manufacturing companies. Between April and June of this year, we discussed various telecommunications technologies, such as analog and digital voice communications carried over copper wire and fiber optic telephone lines; land-line, cellular, and satellite switches; and Personal Communication Services, a technology that could be available in the near future. We also discussed special features, such as call forwarding, voice mail, and speed dialing. (A list of the organizations we met with is attached to this statement).

These discussions revealed that although some technological solutions have been developed to facilitate law enforcement agencies' wiretap efforts, other technology changes have made it more difficult for them to use traditional wiretap methods. While these agencies are still able to conduct most court-approved wiretaps, they have reported problems in effecting wiretaps. Further, they report that investigations were delayed or court orders simply were not pursued because of these problems. For example, the National Technical Investigators' Association, which represents over 3,000 federal, state, and local law enforcement officers engaged in technical investigative activities, reports that "it was almost two years after the introduction of Cellular Telephones before law enforcement had any means to intercept criminal activity conducted on cell phones."[2] In addition, industry representatives told us that there are current and imminent technological situations that would be difficult to wiretap, even though they have not yet received wiretap court orders for those situations.

---

[1] *FBI: Advanced Communications Technologies Pose Wiretapping Challenges* (GAO0/IMTEC-92-68BR, July 17, 1992).

Clearly, there is a need for action that will preserve law enforcement agencies' ability to conduct court-approved wiretaps. Because the details of law enforcement agencies' problems and the specific technological challenges are classified, I cannot elaborate on them in this hearing. However, I would be glad to arrange a separate classified discussion on those topics at your request.

DEFINITION OF LAW ENFORCEMENT REQUIREMENTS HAS IMPROVED

In 1992 we reported that law enforcement agencies had not sufficiently defined their wiretap requirements. Since then, the Federal Bureau of Investigation, in cooperation with other law enforcement personnel, has issued two documents—one in July 1992 and an update in June 1994—describing their capability and capacity requirements. These documents represent considerable effort by law enforcement agencies to delineate their needs.

The capability requirements, which include the timing and nature of information required from wiretaps, making the wiretap undiscernible to the subject of the wiretap, and the reliability and quality of service, are reasonably well defined. The capability requirements include key technical and operational conditions that are needed to conduct wiretaps, and they are often accompanied by helpful clarifications and examples.

On the other hand, the capacity requirement, or quantity and geographic location of simultaneous wiretaps, is not yet precisely defined. Specifically, the June 1994 requirement document states that law enforcement agencies and industry will need to work together to determine the additional capacity that is needed to implement all lawful requests for wiretaps.

COSTS HINGE ON EVOLVING LAW ENFORCEMENT REQUIREMENTS

S. 2375 specifies that the Attorney General, subject to the availability of appropriations, shall reimburse telecommunications carriers for reasonable costs incurred in carrying out the provisions of the bill, and details the nature of the costs that can be reimbursed. The bill authorizes the appropriation of a total of $500 million for fiscal years 1995 through 1998, and authorizes the appropriation of such sums as needed to carry out the bill for fiscal years 1999 and beyond. However, it is virtually impossible to precisely estimate the reimbursement costs discussed in this bill because costs will depend on evolving law enforcement requirements.

For example, even though the capability requirements are reasonably defined, much work remains for industry to identify technological alternatives that will satisfy those requirements across the various technologies. Further, industry must implement those alternatives, which will sometimes involve working with telephone equipment manufacturers. The costs associated with delivering these capabilities can vary widely depending on the technical approaches selected to satisfy the requirements.

More significantly, costs could be affected by how the capacity requirements are defined. S. 2375 suggests basing capacity requirements on characteristics of equipment or service in place, number of subscribers, geographic location, and other factors. If law enforcement requirements demand capacity beyond what is available in current switch technology, then some technology redesign or replacement will be needed to attain the desired capacity levels. Under S. 2375, costs incurred in attaining the desired capacity levels will be subject to reimbursement by the government. These costs will vary greatly depending on how many of the approximately 20,000 land-line switches will need to be replaced to meet the capacity requirements once they are defined.

---

[2] "Digital Telephony and Communications Privacy Act of 1994," National Technical Investigators' Association, April 1, 1994.

Although we cannot precisely estimate total costs associated with this bill, an example may illustrate the way costs could vary. Industry estimates for switch upgrades ranged from $15,000 to about $100,000 per switch, depending on the extent of changes required to the switch hardware and software. In addition, there could be costs to deliver capabilities in technologies other than land-line switches. As a result of this imprecision, the ultimate total cost of meeting this bill's requirements could range from hundreds of millions to billions of dollars.

LAW ENFORCEMENT AND INDUSTRY CAN TAKE STEPS TO CONTROL COSTS

In conducting our discussions, we observed that industry and law enforcement representatives had made considerable progress in communicating with one another since our July 1992 report. Each demonstrated a better understanding of the technologies involved and of each others' concerns. This progress has been facilitated by their voluntary participation on the Electronic Communications Service Provider Committee sponsored by the Alliance for Telecommunications Industry Solutions. We support continued cooperation of law enforcement and industry representatives through this organization, as well as through other means, to identify and resolve problems.

I would like to conclude my remarks with three observations that could help control costs. First, law enforcement and industry representatives should identify known solutions and communicate these to appropriate law enforcement and industry employees across the country. In our discussions with industry representatives, it was clear that some companies had solved problems using equipment that other companies thought was unavailable or were using methods that other companies had not considered. Working cooperatively, the government could avoid reimbursing industry for reinventing solutions that already exist.

Second, law enforcement and industry representatives should work together to identify ways to prioritize and sequence development and deployment efforts needed to satisfy this bill's requirements, to ensure that costs are contained and the most critical law enforcement capability and capacity issues are addressed first. For example, if a switch replacement that is needed to meet a capacity requirement can coincide with a switch replacement to meet a carrier's business needs, then costs could be lowered.

Finally, as provided for in S. 2375, law enforcement agencies need to work with industry to provide law enforcement requirements to the standard-setting organizations, which industry consults in designing telecommunications products and services. Alerting industry to these needs near the beginning of the product development cycle should help lower the costs of meeting law enforcement requirements.

Mr. Chairman, this concludes my remarks. I would be happy to answer any questions you or members of the Subcommittees may have at this time.

ATTACHMENT

LIST OF ORGANIZATIONS CONTACTED BY GAO

Telephone Service Providers

AT&T Company, Bell Atlantic Corporation, BellSouth Corporation, Motorola, NYNEX Corporation, Pacific Telesis Group, Southwestern Bell Corporation, United States Telephone Association, U.S. West Communications.

Manufacturing and Research

AT&T Company, Bell Communications Research, Motorola.

Law Enforcement

Federal Bureau of Investigation, International Association of Chiefs of Police, National Association of Attorneys General, National District Attorneys Association, National Security Council, National Technical Investigators' Association.

Other

Alliance for Telecommunications Industry Solutions.

Senator LEAHY. Thank you.

I would put in the record the letter I sent to Mr. Bowsher on March 24 of this year requesting the study that you are referring to.

[The letter from Senator Leahy to Mr. Bowsher follows:]

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC, March 24, 1994.

Mr. CHARLES A. BOWSHER,
Comptroller General,
General Accounting Office, Washington, DC.

DEAR MR. BOWSHER: I am writing as Chairman of the Senate Judiciary Subcommittee on Technology and the Law to request that the United States General Accounting Office review the Federal Bureau of Investigation's (FBI's) proposal to amend current wiretap laws to ensure law enforcement's capability to conduct court-authorized electronic surveillance in light of advanced telecommunications technology. A copy of the FBI's proposed amendments is enclosed. This proposal differs from proposed legislation circulated by the FBI in 1992 that your office evaluated in a report, dated July 17, 1992.

As part of your review, please evaluate the following aspects of the proposal:

1) *Effect of Proposal on Embedded Telecommunications Systems*—Under the proposal, common carriers must ensure the government's ability to isolate and get concurrent content information "notwithstanding the mobile nature" of the targeted communications or other features used by the subscriber. Please evaluate the extent to which this requirement may force redesigns of the cellular telephone system and current designs for emerging personal communications services (PCS) and other radio frequency-based mobile communications services to permit court-authorized wiretapping. Please include in your evaluation whether redesigns of these systems and services to guarantee wiretapping capability will be as efficient and cost-effective for consumers.
2) *Cost*—Under the FBI's proposal, the government will reimburse common carriers for reasonable and cost-effective charges incurred to comply with new requirements within three years after enactment. The FBI estimates that the cost of retrofitting current telecommunications systems and equipment to meet the proposed requirements is about $500 million, but industry disputes this figure as too low.

Please evaluate the estimated cost of modifying existing networks, services, and features to comply with the FBI's proposed requirements over the next three years, and the costs of incorporating these requirements into future designs for networks, services, and features.

3) *Enforcement Mechanisms*—The FBI's proposal empowers the Attorney General to enforce law enforcement's wiretapping requirements by seeking injunctive relief, $10,000 per day in civil penalties, and by consulting with the Federal Communications Commission for additional sanctions or fines. The proposed requirements are absolute and contain no flexibility for reasonable efforts to comply. Please evaluate whether, because of the penalties, this proposal will effectively give the Attorney General the ability to veto new telecommunications systems or features.

If you have any questions, please do not hesitate to contact Beryl A. Howell at 202–224–3406.

Thank you for your prompt attention to this matter.

Sincerely,

PATRICK J. LEAHY,
U.S. Senator.

Senator LEAHY. I would note regarding the cost estimates for switches, that we should not lose sight of the fact that as technology changes, and it is changing very rapidly in telecommunications, some of these switches would change anyway. It is not simply a case of assuming that under the bill every single switch has to be replaced overnight.

Ms. EDWARDS. That is right.

Senator LEAHY. I think you made that point clear, that as technology changes and switches are being replaced for whatever reason, such as changes in technology, wear, or anything else, this should be taken into consideration.

Mr. Neel, I am delighted to have you here. You and I have worked on telecommunications, privacy and other issues for a long, long time. I am glad to have you here.

STATEMENT OF ROY M. NEEL, PRESIDENT, U.S. TELEPHONE ASSOCIATION

Mr. NEEL. Thank you, Mr. Chairman.

Like Director Freeh and others, I want to thank you and Chairman Edwards and your able staffs in working so hard on this. There has been a lot of time devoted to it. It has been a difficult balancing act and your staff has really done a Herculean job trying to figure all these things out.

It is true that this legislation that you have introduced is a significant improvement over the original administration proposal, particularly in the areas of extending the transition period to 4 years, requiring that the Government reimburse carriers in perpetuity for the costs of expanding capacity to meet law enforcement's needs, improvements in the reasonableness standards, and a number of the privacy considerations. These are all important improvements and we appreciate that.

But as I testified in March, we are still not sure that this kind of legislation is really necessary, beyond, of course, appropriating the kinds of funds that will be necessary for law enforcement to purchase the technical capacity and capabilities from the telecommunications carriers.

Law enforcement authorities already tell us they have the authority to force communications carriers to make these transmissions wiretappable, and as many have said, we have been working with Government to try to figure out these technical solutions. In fact, whether this legislation becomes law or not, this kind of cooperative effort will have to continue.

I think it is important to remember the history of this relationship. We understand there are only about 1,000 court-ordered wiretaps a year, about half of these in New York City's metropolitan area alone, and about a quarter of them involving cellular technology, and half of those in only two States. So the incidence of the demand here is somewhat isolated.

We are concerned that this legislation would create a ubiquitous demand for this technology throughout the country, affecting all manner of compliance problems for telephone companies where there have never been wiretap requests.

Contrary to the testimony, or at least somewhat different from the testimony of the Director, we don't know of any instances where our companies, where telephone companies, have refused to assist law enforcement to accomplish a legal wiretap order. His testimony indicates that they found 183 instances where there have been problems. We may just disagree on the semantics involved. We would very much like to see that list and those examples and try to help work through them, if possible.

Moreover, our companies spend a great deal of money routinely complying with law enforcement requests with no reimbursement. One of our companies alone in an area with only moderate requests spends well over $3.5 million a year routinely meeting these requests.

Our concern with the draft——

Senator LEAHY. Let me just make sure I understand. The $3.5 million is spent by the company with no reimbursement from the law enforcement, Federal, State, or anybody else?

Mr. NEEL. Correct. These are just routine costs of meeting court-ordered compliance.

Our concern with the draft, despite the fact that it is much improved, centers around three main issues. First of all, the scope of coverage. We still think there is a problem in exempting certain types of carriers serving certain kinds of markets. We think that represents some safe harbors for criminals, frankly. If law enforcement believes that is an adequate trade-off to make, there is still the problem of creating a kind of competitive disparity because the technologies that serve those kinds of customers essentially being exempted from these requirements incur fewer costs and represent to customers a more secure network for them. So there is something of a problem there.

We think there needs to be more clarity on the issue of reasonableness——

[Interruption. Coughing by Senator Leahy.]

Mr. NEEL. It's been a tough day.

Senator LEAHY. It's not the testimony. [Laughter.]

Mr. FREEH. You're not allergic to me, are you?

Senator LEAHY. It's that stern look I was getting from Jim Kallstrom back there. [Laughter.]

He's always scared the hell out of me. [Laughter.]

Mr. NEEL. Well, let me go on. We believe there still needs to be further clarity on the reasonableness standards, and essentially what I mean is while the legislation does create safe harbors to a certain extent where companies could deploy technology or consider it without facing fines, we do think there needs to be some clarity to ensure that a company won't face huge problems from law enforcement or that, in using your words, that technology will not be stifled. We think there are still some problems there.

But most important, and I think you have mentioned this, as has Ms. Edwards, we are very worried about the cost reimbursement question. We think that the $500 million estimate of the cost to build capacity and capability in every carrier's network is severely understated. As I noted in March, we believe that it will cost about $1.8 billion to solve the call-forwarding problem alone, and that is only one technology.

We also think it is unrealistic to cap at 4 to 6 years the reimbursement for capability. Essentially, the problem is this. If we take a snapshot right now, you might be able to predict, using services that are on the shelf, what it might cost to make those capable of wiretapping, but we are looking at a very volatile time. Just as if you had looked at the period from 1978 to 1982 and looked at this network, all you would have had to do is go to AT&T and ask for a cost estimate and order something to happen. In 1982, the Government broke up the telephone company and we had an explosion of new services and technologies and all the rules were thrown out.

Right now, across the street, the Senate this morning has taken one further step to blow up the telecommunications system as we know it by injecting more competition, more technological advancement into the network, and we don't have any idea what new products, services, and networks will come into existence.

What this legislation, to a certain extent, and what the administration, we think, has done is look at the nation's telecommunications network using the old traditional model of a local monopoly and local carriers. We don't have that anymore. Already, there are any number of new kinds of telecommunications providers coming into communities and doing new things, some of which would escape the coverage of this.

Moreover, we don't think anyone wants to stifle the development of those things. If you have the fear of a problem, a legal problem, in deploying a new service or technology, the call forwarding of the future, if you will, you are going to be less willing to make massive investments in that if you are facing the very real legal problems of deploying it if there is no technological fix in place.

We also think that despite the belief of some that the cost to local carriers will never be de minimis, after 4, 6, 10, or 20 years. We think these costs will be incurred in perpetuity, not only to increase capacity, the reimbursement of which is covered in this legislation, but to build in the sheer capability of doing that.

We think the legislation also fails to take into account all the other issues that are at work right now in a competitive environment. We think there will be an explosion of new services and we hope those will be taken into consideration. That can essentially be fixed by taking the lid off of the time constraint for reimbursing carriers for putting capability into the networks.

We take these concerns of law enforcement seriously. We want to be part of the solution and we have some suggestions. As I mentioned, I think that the legislation should expand the coverage to include some of these private networks, hospitals, motels and hotels, and so on, the private systems that would otherwise be excluded.

We think you should clarify this reasonableness standard so local carriers, especially small telephone companies, won't fear massive fines and not be forced to install very expensive technology in the out years that they would otherwise not do.

Finally, we think that if you are going to have legislation, that it ought to provide adequate funding and extend the authorization of that funding beyond the 4 to 6 years. Those will make major improvements in legislation that has already improved considerably from the original proposal. Thank you.

[Mr. Neel submitted the following:]

Prepared Statement of Roy Neel on Behalf of the U.S. Telephone Association

USTA, which represents more than 1,100 small, medium and large local exchange telephone carriers throughout the United States, commends Senator Pat Leahy and Congressman Don Edwards for their considerable efforts in working with industry, privacy organizations and law enforcement on this important legislation.

USTA has been an integral force in negotiations leading up to the introduction of this bill. In this regard, members of Judiciary Committee staff, particularly Jim Dempsey and Beryl Howell, have been remarkable for their patience and skill in brokering the many improvements over earlier drafts of this legislation. And we remain fully committed to working with Congress to develop a bill that will stand the test of time.

While this legislation is a considerable improvement over earlier versions, the legislation does not fully satisfy these criteria.

By exempting certain telecommunications providers and networks, the bill is biased against the public switched network. It lacks sufficient protection against unreasonable government requirements. It imposes new cost burdens on the nation's telephone companies, and may curtail investment in and deployment of new network services at a time when investment in the National Information Infrastructure (NII) is a matter of national policy.

IS THIS LEGISLATION NECESSARY?

It is important to note that law enforcement authorities conduct about 1,000 wiretaps a year in the nation. Of those, roughly half are conducted in the New York City metropolitan area. About a quarter are cellular-based, and half of these occur in just two states.

As I testified earlier this year, the *New York Times* reported on March 1, 1994, that documents obtained through the Freedom of Information Act indicated that a survey of several FBI offices found "no instances in recent years in which FBI agents had encountered any technology-based problems in conducting wiretaps." Indeed, where any difficulties have arisen they have been quickly and satisfactorily resolved. (See Digital Privacy and Security Working Group Interim Report, March, 1994, which outlines current law-activities in meeting law enforcement requirements.)

The area of most concern to law enforcement authorities is not in technological barriers to interception, but in capacity limitations in the wireless/cellular environment, where tremendous demand growth has limited the number of ports available to law enforcement for conducting wiretaps.

USTA maintains that legislation is not necessary. Telephone companies consistently have cooperated in good faith with law enforcement, and currently participate in a joint industry and law enforcement standards-setting body which already is addressing surveillance challenges posed by technological advances in telecommunications.

USTA's concerns with this legislation are focused on three areas of the bill: 1) scope of coverage; 2) deployment of new services; and 3) cost recovery.

1. Scope and the Issue of Competitive Neutrality

ALTERNATIVE TELECOMMUNICATIONS PROVIDERS NOT COVERED BY THE BILL

The bill covers only "common carriers," a term which is losing its traditional definition. The term also has different definitions in different states. The concept of limiting the bill to common carriers neglects significant classes of service and service providers who do not fall under the common carrier definition and yet provide competitive alternatives to the services offered by common carriers.

Competitive access providers, shared tenant services, and dozens of other telecommunications service providers compete directly with traditional telephone companies to offer services that look, smell and walk like "plain old telephone service (POTS)."

Every major metropolitan area contains dozens of these alternative telecommunications networks. (See the attachment, "New York City Buildings Connected to Competitive Telecommunications Service Providers.") The World Trade Center, New York Port Authority, University of Michigan, the State of Iowa, office buildings, and hotels—not to mention Internet—are but a few examples of such competitive communications networks. Many of these networks dwarf most of USTA's members' networks.

The millions of users of the Internet could in some cases escape the bill, too, because the bill exempts "free" (i.e., taxpayer financed) private networks. Nearly half of all data traffic in the nation travels over Internet networks. The service is growing by nearly a million users worldwide each month, but significant portions of this traffic are outside the scope of this legislation.

Another class of exempted telecommunications service providers is shared tenant services, which, as described by the FCC, "provide their users with local and interexchange basic service." (Policies Governing the Provision of Shared Telecommunications Services, CC Docket 86–9, *Report and Order,* 3 FCC Rcd 6931. December 6, 1988.)

Yet, they are exempt from coverage under this bill.

We can identify who our competitors are and what their services are today. We cannot predict what new technologies and services will be developed in the future. Nor can we determine exactly how these existing services or their applications will affect the traditional local exchange business. We do know, however, that major segments of the local exchange market—those that carry the highest volumes of traffic and are the most profitable—are being diverted to alternative networks.

To the extent that these alternative services compete with the services offered by local exchange companies, they should be covered in the scope of this legislation.

IS THE BILL COMPETITIVELY NEUTRAL?

In other words, the legislation should not distinguish between one group of service providers and another. If the intent of this legislation is to facilitate government surveillance of electronic communications, then public policy should provide for the government to be able to capture such communications wherever they may be taking place, not just on the traditional local exchange network. Otherwise, steadily increasing amounts of communications that bypass the local exchange network will also circumvent surveillance efforts.

By escaping the requirements of this legislation, these alternative telecommunications networks are given a competitive advantage in both cost and marketing. They do not have to spend considerable sums in modifying equipment or services to comply with the Act. They do not have to be hauled to court or the FCC whenever there is a dispute. They can market their "enhanced security" over public switched network carriers. And security is a major component of consumer confidence, trust and loyalty in choosing a telecommunications provider.

The FBI contends that its "problems" do not lie in these alternative networks; thus, the legislation need not cover these new entrants on the telecommunications scene. But that view embraces an historic perspective. Since the legislation is intended to address future telecommunications technologies, it is important that its coverage also takes a forward-looking view.

LEGISLATION SHOULD COVER SERVICES, NOT "ENTITIES"

USTA continually has proposed language which would apply the requirements of the Act evenly to any service which involves switching or transmission of electronic communications for hire to unaffiliated parties. By applying the bill to services, and not to companies (i.e. common carriers), the bill would attain competitive neutrality.

The Sectional Summary accompanying this bill includes a reference to a functional definition of "local exchange carrier" in Mouse-passed M.R.3636. This support language should be put into the legislative language.

The legislation does provide the FCC with authority to determine when or if an alternative service provider should be covered by the bill, "when such service is a replacement for a substantial portion of the local exchange service and that it is in the public interest to deem such person or entity to be a common carrier for purposes of this Act." (emphasis added.)

But clearly, there's already difference of opinion in interpreting "substantial portion" since many of the above-mentioned networks are not covered.

2. *Reasonableness and deployment of new services and technologies*

Senator Leahy is quoted in the August 10 edition of *Communications Daily* as saying that the goal of this legislation "is to assist law enforcement needs without * * * frustrating the development of new communications technologies or the competitiveness of America's high-tech industry."

But reasonable minds still are debating whether the actual provisions of this legislation accomplish that goal. Doubts still exist as to whether companies can deploy technology that cannot currently be tapped without facing the threat of court action and possible withdrawal of a technology, service or feature.

Even worse, the existence of this potential threat could hinder investment and development efforts in the nation's telecommunications infrastructure. If a company is faced with investing millions of dollars in a new product, but finds in the middle of its development efforts that a surveillance capability will be very difficult—and expensive—to develop, the company may decide to "cut its losses" and abandon an otherwise valuable product development effort.

Further, if a technology is achievable, the bill requires that companies comply with the capabilities requirements. Does this mean that a small telephone cooperative in rural Vermont must modify or retrofit its facilities even though there is little or no likelihood that its surveillance capabilities will ever be needed?

For example, the FBI's REQUIREMENTS document declares law enforcement's desire to "follow" calls through the network to their ultimate destination. This may be possible as an application of advanced intelligent network (AIN) technology, not yet deployed. One conservative estimate of the cost of deploying this feature would be $100 million per region. To support the FBI's requirements, AIN would need to be deployed universally, which is not currently being contemplated.

To satisfy these lingering doubts, the bill must provide a reasonableness standard and not guarantee absolute compliance with law enforcement's requirements. Good faith efforts to comply should be sufficient to find a company in compliance with the Act.

In this regard, it must include economic feasibility as well as law enforcement needs in determining compliance. Again, the Sectional Summary accompanying the bill includes a discussion of economic reasonableness in describing the bill's intent. This language needs to be placed in the legislation itself.

The relative costs and benefits of the bill's requirements placed on all companies must also be a factor in determining compliance. Otherwise, ubiquitous deployment of all "publicly available" capabilities would appear to be required by the bill.

REASONABLENESS AND TIMELY ACTION

The Act states that companies must comply with the capabilities requirements only if: "(i) alternative technologies or capabilities or the facilities of another carrier are not reasonably available * * * and (ii) compliance with the requirements of this chapter is reasonably achievable through the application of available technology * * * or would have been achievable if timely action had been taken." (emphasis added.)

As discussed above, the term "reasonably achievable" leaves much to the imagination, especially without specific reference to economic feasibility or cost-effective deployment considerations. Moreover, what "timely action" should have been taken? There simply is too much ambiguity for determining whether this provision could permit a court retroactively to order a company to withdraw or ban deployment of services or technologies at some time in the future.

Both of these terms need clarification before any company will feel safe investing the considerable money and resources needed to deploy new technologies and services.

RESPONSIBILITY OF MANUFACTURERS

USTA believes that the legislation now requires full cooperation and compliance of manufacturers with the requirements of the Act. Without shared responsibility, it would be possible for a *carrier* to face a court injunction against deploying a new technology or service when a *manufacturer* fails to provide it with the necessary capabilities which may be technologically or economically achievable, just not available.

INTERNATIONAL COMPETITIVENESS

In this global marketplace, what we do in the United States immediately affects market opportunities elsewhere in the world. Barriers to technology or service development here can Significantly affect the competitiveness of American companies vis-a-vis their international competitors.

This legislation effectively forces foreign companies to develop the same surveillance capabilities as AT&T. To the extent that the United States creates unique or expensive requirements for suppliers, it could limit technology alternatives available to American consumers or create offshore opportunities for American companies.

Similarly, what if only one company can develop the capabilities required by the Act? Will carriers be forced to purchase and deploy that company's equipment, regardless of the countless other factors that go into such multi-million dollar decisions?

3. Cost reimbursement

The FBI has estimated (in a "classified" analysis) that the government's costs in reimbursing industry for developing and deploying the modifications necessary to existing facilities to bring them into compliance with law enforcement requirements will be $500 million.

Communications Daily, in an August 4, 1994 article, noted it had obtained the FBI's confidential cost/benefits analysis which demonstrated several flaws. For example, the "FBI figures didn't include cost of upgrading or maintaining switch software and didn't account for new technologies, such as PCS. Nor did it factor in costs that cable companies would have to pay when they began to provide telephone services."

In testimony earlier this year before the House and Senate Judiciary subcommittees, USTA noted that the estimated cost of effecting software changes for call forwarding alone could be as much as $1.8 billion. One large USTA member has estimated that it would cost over $200 million to modify its call forwarding features to accommodate government requirements in this bill. And BellSouth requested a vendor's "inquiry-level" estimate for complying with the FBI's requirements on its wireline business only. The estimate: $138 million to $247 million.

Additional estimates can be made by looking at similar recent network upgrades made to accommodate government requirements to provide equal access to all communications carriers. Two of USTA's members each estimate spending $250 million in this regard. Further, an August 5, 1994 Communications Daily article notes that the FCC has estimated that implementing another government mandate—for enabling customers to chose their long distance carrier automatically from pay phones—will cost $1.8 billion.

In short, $500 million, as far as we can tell, will not even come close to the mark. USTA's principal concern with this legislation, therefore, is what happens when, or if, the $500 million fails to cover the costs of complying with the government's requirements.

"GOLDPLATING"

The record for government cost reimbursement for existing law enforcement activities does not give cause for great comfort with industry members, either. One USTA member company, with only moderate law enforcement obligations, spends $3.7 million a year accommodating over 100,000 law enforcement subpoenas, many of which require boxes of documentation.

These expenditures of time and personnel are borne by the company alone, without government reimbursement, even though the company frequently requests compensation for its efforts.

One can only presume that obligations are only a fraction of those imposed on such companies where law enforcement activity is more concentrated.

And, perhaps because there is no mechanism that limits government's "free" access to any information it wants, its demands for customer information have been increasing dramatically on an annual basis.

In fact, in June of this year, at least one of USTA's large company members received a subpoena from the Drug Enforcement Agency requesting "the identity of published and unlisted [presumably meaning nonpublished numbers] residential and business telephones * * * by area code, and telephone number, together with first name, last name (company name), address, city and state for all published and unlisted residential and business telephones in the service area * * *" (See attachment.)

Besides the sheer audacity of this request, and its obvious implications regarding privacy and security of innocent American citizens, there naturally was no offer to compensate the company for complying with the Agency's demands, despite the fact that commercially available data bases (purged of nonpublished numbers) exist on the market today.

There must be a mechanism for preventing the government from making excessive demands, when a more modest and less expensive solution may satisfy most of the government's objectives.

THE OPPORTUNITY COSTS OF SURVEILLANCE REQUIREMENTS

It should be noted that whatever costs are being discussed, they represent time, effort, investment, research, and implementation of capabilities to meet government demands. There is no market incentive or cost recovery involved in developing such capability. That is, companies do not benefit from installing surveillance capabilities. (In fact, there are market disincentives if one takes into account the fact that companies are being required to build the ability to compromise security into their networks.)

To the extent that such time and investment is dedicated to meeting law enforcement's surveillance demands, and not developing advances in network enhancements for the improvement of private and commercial communications capabilities, then this Act has to be measured in terms of its opportunity costs; i.e., resources lost or diverted from other pursuits.

This is not to say that there are not significant societal benefits to meeting law enforcement demands. But the relative social benefits of law enforcement objectives need to be weighed against the costs of compliance.

FOUR (OR SIX) YEAR COMPLIANCE DEADLINE

Coming up with new features is no easy feat. Developing standards alone takes time, human effort and resources, and money. Even then, standards are only the beginning of a continuum which can last for years before eventually resulting in the deployment of new features or services in a manner that ensures their interoperability with existing network facilities.

To illustrate, after standards are developed, the following steps must be taken:

1) Develop technical requirements or specifications—to 24 months;
2) Solicit industry input and finalize the requirements—6 to 12 months);
3) Vendor implementation—9 to 24 months
4) Trial and testing to determine actual viability and interoperability with existing network facilities and features;
5) Deployment (subject to cost/benefit analysis and funding availability);
6) Operation and maintenance.

Much of this process is not within the control of telephone companies, particularly as more and more services and features are a function of central office switching equipment.

It is clear to USTA members that there is both insufficient funding and quite possibly unreasonable time requirements in this legislation to cover the substantial costs and efforts needed to comply with the Act even within the first four years following its enactment.

COSTS AFTER FOUR YEARS

It is not reasonable to assume that costs will, as alleged by the FBI, be merely "de minimis" after four years.

Costs associated with developing and deploying new features simply are not "de minimis." As with the development of any feature, it takes time and money to meet additional requirements, particularly requirements as complex as those being posed by the FBI. And to the extent that this legislation develops a market for noncovered communications providers in a competitive environment, these costs will discriminate against carriers and their customers and investors.

In other words, there is and will be a continuing need to develop new standards as new technologies are introduced and features, functions and other applications are built around the new technology platforms.

An additional safeguard needs to be added to the bill to prevent the government from seeking modifications it could not obtain during the first four years (of six, if an extension is granted) after enactment.

The legislation commits the government to paying for increased *capacity* costs indefinitely. This provision should apply to *capability* compliance costs, as well, and should include the costs of operating and maintaining these government-imposed capabilities.

A SURVEILLANCE BUDGET: "PAY-AS-YOU-GO"

If it is only for the first four years that the government is given its $500 million authorization, then nothing in the bill prevents the government from asking a company in the fifth year after enactment to modify its facilities to comply with the Act's requirements.

To prevent retroactive application of the requirements, the legislation should clarify that the government cannot come back to a company in the fifth year, or later, and demand compliance for that which it could not afford, or did not properly plan for during the first four years.

What is needed is a means to prevent government from making unlimited demands at the expense of the American consumer. In short, government needs cost containment incentives.

This can be accomplished by strictly limiting law enforcement demands to the amount ($500 million) authorized in this Act. Companies should be found in compliance with the Act if the government fails to reimburse them. In other words, the requirements of the Act should not attach to the company, its customers and its shareholders.

The $500 million authorized for the government's implementation of the Act thereby would become a "surveillance budget" under which law enforcement would be forced to develop appropriate priorities and reasonable requirements. If, in fact, the government's estimated cost of compliance is $500 million, then it should be able to accomplish all of its objectives within this budget. If, however, $500 million is too small an amount, then the government will need to determine where and how best to spend its budget.

There are several advantages to this approach. First, it prevents "goldplating." Law enforcement will have to concentrate its efforts where they are needed most, rather than ask for ubiquitous capability deployment where there may be little or no need. Pay-as-you-go will force the government either to limit its spending requests or modify its technical requirements.

Second, consumers will not be burdened from attempts to pass through significant costs associated with unreimbursed government requirements. This becomes even more problematic in the changing regulatory environment facing telephone companies today. The introduction of competition into telecommunications markets undermines a carrier's ability to recover nonmarket costs—such as surveillance costs—from its customers.

Third, small companies will be disproportionately affected by the costs of complying with this Act. Most USTA members can ill-afford million dollar fixes (that may be considered under the Act as "reasonable") for building capabilities that may never be used.

Fourth, USTA noted in its testimony earlier this year that a poll conducted by Yankelovich Partners in March and reported in Time Magazine found that "two-thirds of Americans said that it was more important to protect privacy of phone calls than to preserve the ability of the police to conduct wiretaps." By limiting government surveillance appropriated funds, Americans will know as a matter of public record exactly how much the government is spending on surveillance activities.

This "pay-as-you-go" solution should be applied to all capabilities and capacity requirements after four years following enactment, as well.

REIMBURSEMENT PROCEDURES

Companies need assurance the government will pay for what it demands. This legislation gives the FCC authority to settle any disputes that may arise in debating "reasonable costs" to be reimbursed by the government. But the timing of payment remains in question. The Act should ensure that companies need not comply until or unless they are paid.

This bill also contains a provision granting the Attorney General authority "to establish any procedures and regulations deemed necessary to effectuate timely and cost-efficient reimbursement * * *" At least two USTA member companies are victims of nonpayment of long-outstanding bills.

USTA recommends adding language to this provision that ensures a process by which industry has an opportunity to effect these regulations, and that requires issuance of such regulations in a timely manner.

WHY SHOULD THE GOVERNMENT PAY?

Some argue that the government has no obligation to compensate private industry at all for meeting social obligations.

First, as noted above, there is no consumer advantage or market value to building surveillance capabilities into telecommunications equipment. Reimbursement is not paying for some corporate benefit. It is paying for the government's law enforcement requirements, a legitimate taxpayer expense.

Second, as noted above, imposing significant cost obligations on companies of vastly different sizes and financial capabilities would impose substantially disproportionate economic burdens.

Third, because the bill as introduced fails to treat all telecommunications service providers equally, failure to compensate those companies covered by the bill will cause substantial competitive advantages for those companies not obligated to comply with and pay for law enforcement requirements.

Fourth, as aforementioned, failure to compensate for government surveillance activities effectively hides the government's expenditures from public scrutiny.

Finally, a government obligation to pay for what it demands, under strict budgetary constraints, prevents it from "goldplating" its demands.

THE AUSTRALIA EXAMPLE

With the introduction in 1991 of competition in its telecommunications market, the Australian government granted to carriers the right to charge for assistance they provide to police authorities.

The government's decision was based on the following factors:

1) When Telecom Australia was a government monopoly, charging for surveillance meant the government in effect was charging itself for surveillance costs.
2) With the introduction of competition, the government considered it unfair to the shareholders of those companies that they should bear the costs of government requirements.
3) Because of the size discrepancy between Telecom Australia and the new entrants, the government also considered it unfair to impose a higher relative cost on smaller companies.
4) The government determined costs should be visible to the public so that an assessment can be made about whether the costs of a particular service or facility are worth the benefit derived from those services or facilities.
5) Police authorities had been accused of having no incentive for efficiency or cost containment.

Accordingly, the federal government determined that the most "economically efficient" and "socially beneficial" means of dealing with police authority requests for intercept facilities was to ensure "full transparency," and the general body of taxpayers carried the costs of those facilities through the budgets of the police authorities.

The government also prohibited the introduction of new technologies which were not capable of interception. This prohibition caused significant negative effects on product development in that nation's telecommunications system. For example, with overloaded analogue mobile telephone capacity, the government was anxious to develop and deploy new GSM-based mobile technology. However, the new technology was untappable.

Consequently, the government authorized the carriers to deploy the new GSM networks, while requiring them to work "double time" to develop an interception capability.

Meanwhile, the Minister of Communications initiated a review to investigate concerns of law enforcement authorities about their obligation to reimburse carriers. The review reaffirmed the basic principles outlined above that the costs of intercept facilities should be borne by the taxpayers. The government also recommended that equipment providers be brought "into the loop" to give realistic and reasonable estimates for needed technology.

USTA RECOMMENDS THE FOLLOWING CHANGES TO THIS LEGISLATION

1. Scope

The bill should cover all telecommunications services, rather than "carriers." Reference to a functional definition of "local exchange carriers" in House-passed H.R. 3636 is given in the Sectional Summary accompanying the bill. This definition should be made part of the legislative language. Any transmission or switching of electronic communications to unaffiliated parties for hire is a telecommunications service.

2. Reasonableness

Ensure that good faith efforts to comply with the requirements of the Act are sufficient grounds for compliance.

Put into the legislative language the Sectional Summary discussion of *economically feasibility* as a criterion of compliance.

Delete reference to "timely action" that should have been taken. Alternatively, the bill must state that a *good faith* effort to develop economically and technologically achievable standards that are *intended to satisfy* law enforcement requirements is sufficient to allow deployment of technologies or services that may not contain surveillance capabilities.

Add a provision which requires reasonable law enforcement demands which may be "achievable" but have little likelihood of being required.

3. Costs

Establish "pay-as-you-go" provision which ensures that the government has only that which is appropriated for purposes of this Act with which to modify existing network facilities. Companies not reimbursed under such appropriated funds shall be found in compliance with the Act.

Expand reimbursement authority after four years to include reimbursement for capabilities as well as capacity requirements. Provide same stipulation that modifications companies not reimbursed shall be in compliance with the Act.

Establish requirement for timely payment and promulgation of reimbursement procedures with industry input.

CONCLUSION

Telephone exchange companies will, as they consistently have in the past, endeavor in good faith to meet the requirements of the law enforcement community. In developing a bill that will ensure law enforcement's legitimate demands in conducting surveillance activities with future telephony technologies and services, the United States must ensure that a standard of reasonableness guide its actions.

It is important to remember that there are about 1,000 wiretaps performed each year in the United States. The government intends to spend about $125,000 par wiretap per year for the next four years, if it sticks to its budget.

While industry is willing to facilitate the objectives of law enforcement whenever feasible, we cannot afford to raise barriers to investment in and development of new telecommunications technologies and services.

Finally, USTA again acknowledges the efforts of Senator Leahy and Congressman Edwards and their staffs for their willingness to draft legislation that meets the test of time.

I thank the committee for allowing USTA to testify. I look forward to continuing the process of improving this Act to that it can meet the interests of the local exchange industry while satisfying the objectives of our nation's law enforcement community.

New York City Buildings Connected to Competitive Telecommunications Service Providers

560 First Ave
350 5th Ave
666 5th Ave
122 5th Ave
452 5th Ave
522 5th Ave
787 7th Ave
810 7th Ave
888 7th Ave
747 10th Ave
811 10th Ave
32 Ave of the Americas
100 Ave of the Americas
1100 Ave of the Americas
1133 Ave of the Americas
1155 Ave of the Americas
1185 Ave of the Americas
1221 Ave of the Americas
1251 Ave of the Americas
1271 Ave of the Americas
1285 Ave of the Americas
1290 Ave of the Americas
1301 Ave of the Americas
1330 Ave of the Americas
1345 Ave of the Americas
1370 Ave of the Americas

4 Albany Street
1 Bankers Trust Plaza
101 Barclay St
1 Battery Park Plaza
17 Battery Place
15 Broad St
20 Broad St
30 Broad St
40 Broad St
50 Broad St
60 Broad St
61 Broad St
67 Broad St
80 Broad St
85 Broad St
90 Broad St
104 Broad St
125 Broad St
116th & Broadway
2 Broadway
25 Broadway
26 Broadway
45 Broadway
55 Broadway
61 Broadway
120 Broadway

New York City Buildings Connected to Competitive Telecommunications Service Providers

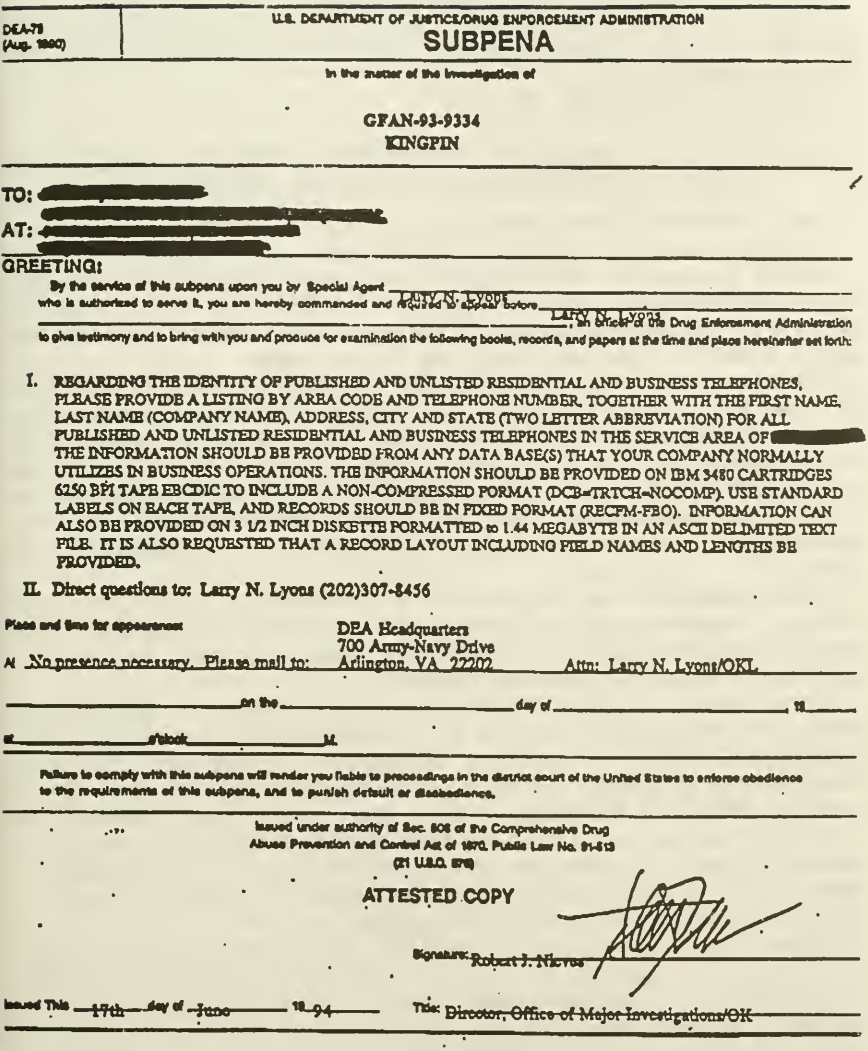
140 Broadway
195 Broadway
222 Broadway
233 Broadway
250 Broadway
270 Broadway
305 Broadway
770 Broadway
825 Broadway
1633 Broadway
1675 Broadway
1700 Broadway
1775 Broadway
45 Broadway Atrium
1 Centre St
100 Centre St
1 Chase Plaza
100 Church St
250 Church St
22 Cortlandt St
227 E 19th St
120 E 23rd St
150 E 42nd St
250 E 42nd St
345 E 46th St
12 E 49th St
10 E 50th St
55 E 52nd St
153 E 53rd St
525 E 68th St
1 Exchange Place
20 Exchange Place
26 Federal Plaza
1 Financial Square
866 First Ave
111 Fulton St
100 Gold St
390 Greenwich St
7 Hanover Sq
10 Hanover Sq
60 Hudson St
325 Hudson St
375 Hudson St
90 John St
116 John St
127 John St
130 John St
405 Lexington Ave
420 Lexington Ave
425 Lexington Ave
466 Lexington Ave
33 Liberty St

New York City Buildings Connected to Competitive Telecommunications Service Providers

1 Libery Plaza
Merrill Lynch
130 Liberty Plaza
33 Liberty St
200 Liberty St
1 Madison Ave
51 Madison Ave
535 Madison Ave
590 Madison Ave
625 Madison Ave
33 Maiden Lane
59 Maiden Lane
100 Maiden Lane
180 Maiden Lane
1 New York Plaza
2 New York Plaza
4 New York Plaza
32 Old Slip
1 Park Ave
200 Park Ave
237 Park Ave
245 Park Ave
277 Park Ave
299 Park Ave
320 Park Ave
399 Park Ave
1 Park Ave Plaza
75 Park Place
180 Park Place
399 Park Place
375 Pearl
2 Penn
4 Penn
11 Penn
4 Pennsylvania Plaza
5 Pennsylvania Plaza
20 Pine St
70 Pine St
80 Pine St
88 Pine St
40 Rector St
1 Rockefeller Plaza
30 Rockefeller Plaza
50 Rockefeller Plaza
75 Rockefeller Plaza
1 State St Plaza
33 Thomas St
85 Trinity Pl
86 Trinity Pl
1 United Nations Plaza
200 Vesey
250 Vesey

New York City Buildings Connected to Competitive Telecommunications Service Providers

40 W 23rd St
460 W 33rd St
114 W 47th St
125 W 50th St
31 W 52nd St
51 W 52nd St
40 W 53rd St
524 W 57th St
555 W 57th St
250 W 57th St
47 W 66th St
77 W 66th St
1 World Financial Center
2 World Financial Center
3 World Financial Center
1 World Trade Center
2 World Trade Center
4 World Trade Center
5 World Trade Center
6 World Trade Center
7 World Trade Center
1 Wall St
14 Wall St
30 Wall St
40 Wall St
60 Wall St
75 Wall St
100 Wall St
111 Wall St
120 Wall St
10 Washington
570 Washington
55 Water St
77 Water St
175 Water St
199 Water St
19 West St
140 West St
125 West End Ave
1 Western Union Intl Plaza
1 Whitehall St
33 Whitehall St
90 William St
100 William St
110 William St
170 William St
1275 York



DEA-79
(Aug. 1990)

U.S. DEPARTMENT OF JUSTICE/DRUG ENFORCEMENT ADMINISTRATION

SUBPENA

In the matter of the investigation of

GFAN-93-9334
KINGPIN

TO: [redacted]

AT: [redacted]

GREETING:

By the service of this subpena upon you by Special Agent Larry N. Lyons who is authorized to serve it, you are hereby commanded and required to appear before Larry N. Lyons, an officer of the Drug Enforcement Administration to give testimony and to bring with you and produce for examination the following books, records, and papers at the time and place hereinafter set forth:

I. REGARDING THE IDENTITY OF PUBLISHED AND UNLISTED RESIDENTIAL AND BUSINESS TELEPHONES, PLEASE PROVIDE A LISTING BY AREA CODE AND TELEPHONE NUMBER, TOGETHER WITH THE FIRST NAME, LAST NAME (COMPANY NAME), ADDRESS, CITY AND STATE (TWO LETTER ABBREVIATION) FOR ALL PUBLISHED AND UNLISTED RESIDENTIAL AND BUSINESS TELEPHONES IN THE SERVICE AREA OF [redacted] THE INFORMATION SHOULD BE PROVIDED FROM ANY DATA BASE(S) THAT YOUR COMPANY NORMALLY UTILIZES IN BUSINESS OPERATIONS. THE INFORMATION SHOULD BE PROVIDED ON IBM 3480 CARTRIDGES 6250 BPI TAPE EBCDIC TO INCLUDE A NON-COMPRESSED FORMAT (DCB=TRTCH=NOCOMP). USE STANDARD LABELS ON EACH TAPE, AND RECORDS SHOULD BE IN FIXED FORMAT (RECFM-FBO). INFORMATION CAN ALSO BE PROVIDED ON 3 1/2 INCH DISKETTE FORMATTED to 1.44 MEGABYTE IN AN ASCII DELIMITED TEXT FILE. IT IS ALSO REQUESTED THAT A RECORD LAYOUT INCLUDING FIELD NAMES AND LENGTHS BE PROVIDED.

II. Direct questions to: Larry N. Lyons (202)307-8456

Place and time for appearance:

At No presence necessary. Please mail to: DEA Headquarters
700 Army-Navy Drive
Arlington, VA 22202 Attn: Larry N. Lyons/OKL

________ on the ________ day of ________, 19____

at ______ o'clock ______ M.

Failure to comply with this subpena will render you liable to proceedings in the district court of the United States to enforce obedience to the requirements of this subpena, and to punish default or disobedience.

Issued under authority of Sec. 506 of the Comprehensive Drug Abuse Prevention and Control Act of 1970, Public Law No. 91-513 (21 U.S.C. 876)

ATTESTED COPY

Signature: Robert J. Nieves

Issued This 17th day of June 19 94

Title: Director, Office of Major Investigations/OK

Representative EDWARDS. Thank you very much, Mr. Neel.

The next member of the panel to testify is Thomas E. Wheeler. Mr. Wheeler is President of the Cellular Telecommunications Industry Association.

You may proceed, Mr. Wheeler.

STATEMENT OF THOMAS E. WHEELER, PRESIDENT, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Mr. WHEELER. Thank you very much, Mr. Chairman.

We appreciate the opportunity to be here before you today, particularly because we were kind of the poster child of the last hearing when everybody was talking about cellular as the example of some of the new telecommunications technologies that require some of the changes we are talking about today.

One retrospective on that hearing. It is interesting to note that by the FBI's own estimate, the cellular industry, which today serves approximately 5 percent of the population, was responsible for 25 percent of the wiretaps in 1993. I just put that forward as a physical manifestation of our commitment to addressing the issues of court-authorized surveillance and our recognition of our responsibility to provide both the capability and the capacity to do that.

This legislation, as everybody else has previously said, is a significant improvement over the previous draft, and again, cudos need to be extended to the staffs of these committees, to the FBI, and to the other industries involved.

There are four principal wireless-related issues in the current draft of the legislation, and let me just address those quickly.

One is that the bill outlaws the ability to steal someone else's electronic code in order to impersonate another user of the wireless service. We have all heard stories about people with humongous cellular bills because somebody had snatched their electronic code out of the air, cloned that into another phone, and was charging phone calls to Colombia or wherever onto their phone. Amazingly, that is not an illegal act. This bill makes it so.

That is very significant, because not only is this a crime against consumers and against the providers of wireless services, but also if you have a situation where there is floating around out there multiple users of the same electronic serial numbers, you don't know who you are tapping. You have three or four or five options and they say, hello, I am this one person, but they may not really be. So that change in the law not only helps protect consumers but also is a linchpin into making wireless court-authorized surveillance possible.

The second provision in the bill is the establishment of requirements and procedures for wiretaps in a wireless environment. This deals with the two C's, if you will, capability and capacity.

First, you have to have the capability technically to be able to get the desired information. There is underway right now, through an organization called the Electronic Communications Service Providers Committee, joint efforts of carriers, law enforcement, and manufacturers to come up with the standards for those kinds of technical capabilities. This bill recognizes that kind of process and provides appropriate review procedures, but I am happy to say that that is underway and a long way down the track.

However, the capacity issue, the number of simultaneous taps, is a matter which is not so easily standardized and to which the kind of process which worked on capability may also want to be applied. I will withhold further discussion of that for 1 more minute while I discuss the third wireless related component of this legislation.

That third component is that it is a recognition that what we are talking about is an industry-wide effort that must involve not only carriers but also the suppliers and manufacturers who enable the service. Simply put, if they don't build it, we can't do it and we have to be a team in this whole exercise.

The shortcoming in this bill is that, as Ms. Edwards and others have said, the cost is unknown because the capacity and capability requirements are unknown. So we would suggest that there might be a way of addressing that. Obviously, the key to the cost question is a capacity question. The more capacity, the greater the cost. We know that in Topsham, VT, the capacity is different than in New York City in terms of the requirement levels, but how different?

The bill says, well, relax, the Attorney General is going to tell you how different after consultation with the appropriate parties. We would specifically submit that consultation isn't enough, that what is needed is the discipline of an on-the-record proceeding. Human nature being what it is, it is important to differentiate between what is really necessary and what is requested.

We all go through, personally and in corporate lives and elsewhere, the differentiation between wants and needs. The way that works best in a governmental environment is in a formal rulemaking where the parties put information on the record and then challenge each other's assumptions and there is a conclusion which is based on a formal procedure, not just an informal consultation. We believe that the taxpayers deserve that kind of disciplined consideration of their financial exposure.

Therefore, we would suggest that we work together to catch crooks and to save taxpayers' money without delaying the process by focusing on adding a formal procedure as a substitute for the informal activity which will determine the capacity needs to be established by the Government.

To both of the chairmen and to the Director, we reiterate our gratitude for the manner in which you have been sensitive and responsive to the issues that we have raised throughout the discourse of this debate and we look forward to working further with you on these additional changes.

[Mr. Wheeler submitted the following:]

PREPARED STATEMENT OF THOMAS E. WHEELER ON BEHALF OF THE CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION

I. INTRODUCTION

The commercial mobile wireless telecommunications industry appreciates the opportunity to appear before you today to discuss our industry's involvement in meeting law enforcement's surveillance requirements.

The Cellular Telecommunications Industry Association ("CTIA") was organized in 1984. Over the past ten years its membership has grown to encompass all aspects of two-way wireless telecommunications (known as "commercial mobile service"), including licensed cellular, personal communications services, and enhanced specialized mobile radio. The association also counts as members the wireless service providers in Canada and Mexico, equipment and infrastructure manufacturers, and others with a general interest in the wireless industry.

The wireless decade began with pioneers from both large and small companies taking risks to create a nationwide cellular network. Private entrepreneurs have invested almost $14 billion in wireless infrastructure. Today, more than 300 cellular carriers provide service to over 16 million Americans in every one of the nation's 734 metropolitan and rural service areas. As of December 1993, almost 40,000 people are directly employed by the cellular industry; another 125,000 are employed in related industries.[1] In less than ten years of operation, the cellular industry has created over 165,000 jobs for Americans.

EXHIBIT I

II. HOW WIRELESS WORKS

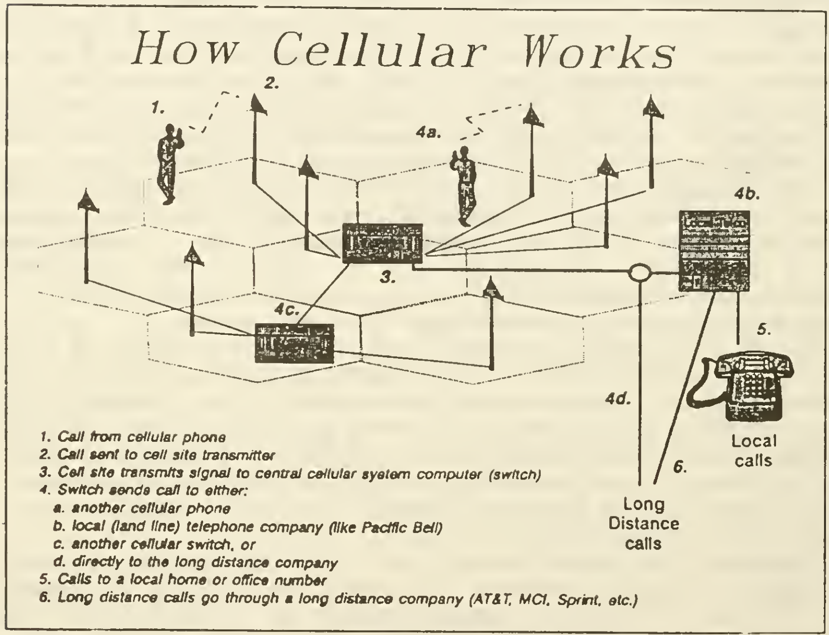

How Cellular Works
1.
2.
4a.
4b.
3.
4c.
5.
4d.
6.
Local calls
Long Distance calls
1. Call from cellular phone
2. Call sent to cell site transmitter
3. Cell site transmits signal to central cellular system computer (switch)
4. Switch sends call to either:
a. another cellular phone
b. local (land line) telephone company (like Pacific Bell)
c. another cellular switch, or
d. directly to the long distance company
5. Calls to a local home or office number
6. Long distance calls go through a long distance company (AT&T, MCI, Sprint, etc.)

Exhibit I

When a subscriber makes a call on a wireless phone, as shown in Exhibit I, radio waves are transmitted to the nearest tower. By constructing the network using small, low power cells, wireless technology reuses the same radio frequencies and, thus, can handle a large number of simultaneous users. Instead of having a radio channel, like Citizen's Band radio, that reaches across a market and must be shared by everyone, low power, limited reach wireless cells permit the channel to be used again and again. The ability to travel between cells is achieved by a sophisticated signal strength monitoring and computer control system which senses when a caller is leaving a cell and hands that call off to an adjacent cell.

Once the communications signal is received at the cell tower, the "wireless" component of the transmission is over and more traditional technologies take over. From the cell tower the system transfers the call to the mobile telephone switching office ("MTSO"). The MTSO is the wireless system's equivalent of the landline local exchange central office switch. At the MTSO, the subscriber's connection is monitored by wireless messages to and from the subscriber's unit on a control channel separate from the voice channel. The MTSO reads the information contained in the control channel and, depending upon the information received, routes the subscriber's call to the public switched landline network, a long distance carrier, or to another mobile unit in the service area. Exhibit I, *see supra,* illustrates how a wireless call is transmitted.

---

[1] CTIA Data Survey, "The Wireless FactBook," March 1994.

If a subscriber travels beyond the home carrier's geographic area and makes calls on his/her wireless phone, the local carrier in *that* market will provide the service. This is known as roaming. Wireless carriers allow their customers to use each other's service by executing carrier-to-carrier roamer agreements. These agreements mainly specify which services each carrier will offer roamers, and how the carriers will exchange information to permit timely and concise billing for services rendered on each carrier's system.

The billing information exchanged between carriers passes through a series of industry standardized edits, ensuring that billing information which appears on a subscriber's bill is consistently timely, error-free and easy to understand. Each carrier submits it's own figures for revenue owed and due through a central bank, which in turn performs a net financial settlement process. CIBERNET Corporation, a subsidiary of CTIA, administers this program of net settlements for the industry.

EXHIBIT II

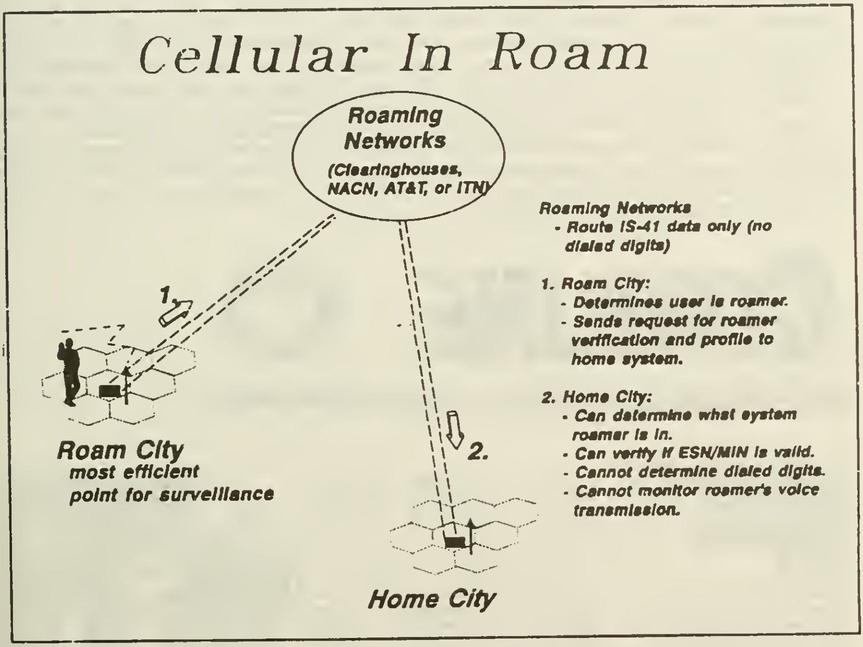

Cellular In Roam
Roaming Networks
(Clearinghouses, NACN, AT&T, or ITN)
Roaming Networks
- Route IS-41 data only (no dialed digits)
1. Roam City:
- Determines user is roamer.
- Sends request for roamer verification and profile to home system.
2. Home City:
- Can determine what system roamer is in.
- Can verify if ESN/MIN is valid.
- Cannot determine dialed digits.
- Cannot monitor roamer's voice transmission.
1.
2.
Roam City
most efficient point for surveillance
Home City

Exhibit II

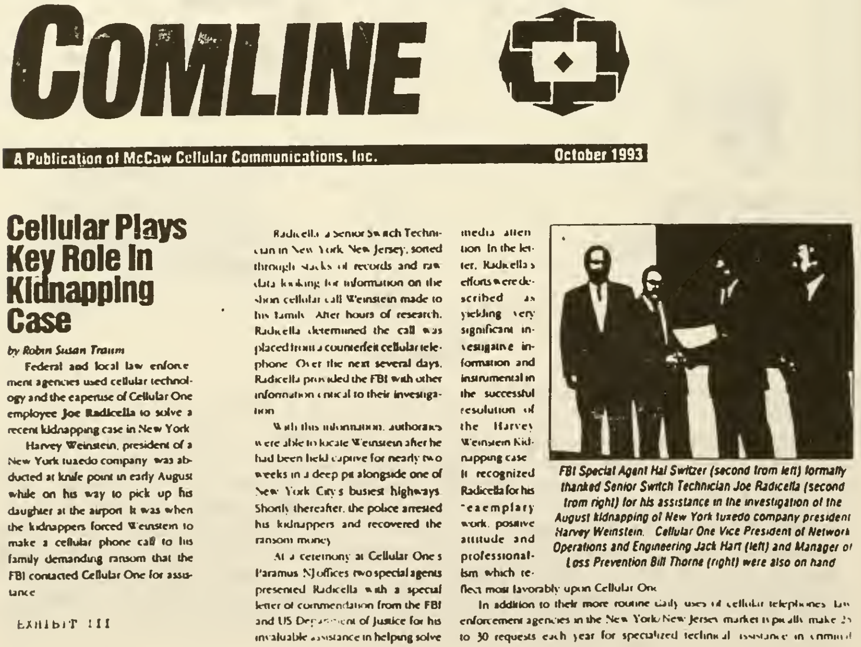
Roaming connections are more challenging than calls made within the home system. But today, thanks to roaming agreements and the IS–41 signaling protocol, subscribers can use their telephones throughout the nation. The IS–41 technology is particularly important in a law enforcement context because it permits systems to send data to each other regarding a specific call. Exhibit II illustrates how, when a wireless phone is turned on and registered in a roaming market, an IS–41 message is automatically sent to the home system. This message asks if it is okay to provide service to the phone and what special services or features the subscriber uses. The IS–41 message then permits the home MTSO to route calls to the subscriber in the roaming market.

III. WIRELESS INDUSTRY SUPPORT OF LAW ENFORCEMENT

The wireless telecommunications industry is relatively young, and one which has experienced explosive growth after its "start from scratch." No less an expert than AT&T, the developer of cellular technology, forecast that by the year 2000 there would be only 900,000 cellular subscribers. In its early years, the challenge was to survive and make the technology work. The wireless industry's pervasive impact on society is a relatively new development which has brought with it uses for ill, as well as innumerable uses for good.

With such an impact on society goes responsibility, in this case the responsibility to look beyond survival and technology to the role of the industry in the community. This includes the responsibility to support law enforcement's ability to lawfully intercept wireless communications. The wireless industry has assumed its responsibility to law enforcement. Cellular carriers were utilized in the execution of nearly 25 percent of the FBI's estimated 976 electronic surveillance court orders executed at the federal and state levels throughout the nation in 1993.[2]

Twenty-five percent of all wiretaps is illustrative of how the wireless industry has been responsive in the manner m which it has supported law enforcement. Unfortunately, for security reasons law enforcement typically asks carriers not to discuss their success in call interdiction. Thus, it is difficult to portray the many successful instances of joint cellular-law enforcement efforts which exist. Occasionally, however, one story does find its way into the press and, then, can be discussed. One such story is how a cellular company's prompt action saved a life and resulted in a special citation from the FBI. Working with law enforcement, Cellular One in New York, used wireless intercept technology to assist the FBI in apprehending the kidnappers of Harvey Weinstein, the New York clothier who was kidnapped for ransom and buried alive. The cellular carrier was able to determine where the victim was located after his captors forced him at knife point to make a short cellular telephone call to his family to demand ransom money. Cellular One was not only able to record the call detail, but was also able to determine from where the call was placed. During the two-week investigation, critical investigatory information was obtained by the FBI through the cellular network. This information led to the rescue of the kidnap victim, the arrest of the kidnappers, and the recovery of the ransom money. Exhibit III is a reproduction of a news article reporting on this story, including an award of recognition presented by the FBI.



COMLINE

A Publication of McCaw Cellular Communications, Inc. October 1993

Cellular Plays Key Role In Kidnapping Case

by Robin Susan Traum

Federal and local law enforcement agencies used cellular technology and the expertise of Cellular One employee **Joe Radicella** to solve a recent kidnapping case in New York.

Harvey Weinstein, president of a New York tuxedo company, was abducted at knife point in early August while on his way to pick up his daughter at the airport. It was when the kidnappers forced Weinstein to make a cellular phone call to his family demanding ransom that the FBI contacted Cellular One for assistance.

Radicella, a Senior Switch Technician in New York/New Jersey, sorted through stacks of records and raw data looking for information on the short cellular call Weinstein made to his family. After hours of research, Radicella determined the call was placed from a counterfeit cellular telephone. Over the next several days, Radicella provided the FBI with other information critical to their investigation.

With this information, authorities were able to locate Weinstein after he had been held captive for nearly two weeks in a deep pit alongside one of New York City's busiest highways. Shortly thereafter, the police arrested his kidnappers and recovered the ransom money.

At a ceremony at Cellular One's Paramus NJ offices two special agents presented Radicella with a special letter of commendation from the FBI and US Department of Justice for his invaluable assistance in helping solve the kidnapping that drew national media attention. In the letter, Radicella's efforts were described as yielding very significant investigative information and instrumental in the successful resolution of the Harvey Weinstein Kidnapping case. It recognized Radicella for his "exemplary work, positive attitude and professionalism which reflect most favorably upon Cellular One."

In addition to their more routine daily uses of cellular telephones, law enforcement agencies in the New York/New Jersey market typically make 25 to 30 requests each year for specialized technical assistance in criminal investigations. ■

FBI Special Agent Hal Switzer (second from left) formally thanked Senior Switch Technician Joe Radicella (second from right) for his assistance in the investigation of the August kidnapping of New York tuxedo company president Harvey Weinstein. Cellular One Vice President of Network Operations and Engineering Jack Hart (left) and Manager of Loss Prevention Bill Thorne (right) were also on hand

EXHIBIT III

It is not only right that wireless providers should assist law enforcement in this way, *it is the law*. In a 1970 amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Congress enacted a provision specifying that a "communication common carrier * * * shall furnish the government applicant for court-ordered electronic surveillance with all information, facilities, and technical assistance necessary to accomplish the interception."[3] While the current law is clear, unambiguous and working, the wireless industry fully understands the concerns expressed by the FBI of the need to keep law enforcement agency capabilities current with new technology in the rapidly evolving telecommunications industry.

---

[2] Source: Administrative Office of the United States Court, Wiretap Report, January 1–December 21, 1993. See attachment A.

The telecommunications industry, including the wireless industry, has continued to work closely with the law enforcement community to resolve technical and electronic surveillance problems. As further evidence of this cooperation, in March 1993, the Board of Directors for the Alliance for Telecommunications Industry Solutions, (ATIS), formerly the Exchange Carrier Standards Association, (ECSA), approved a request from the industry and law enforcement agencies to sponsor a committee to identify those technical and associated operational issues related to lawfully authorized electronic surveillance and to develop resolutions to such issues for voluntary implementation by the industry. That committee is the Electronic Communications Service Provider (ECSP) Committee.

ATIS is a not-for-profit corporation, established for the purpose of promoting timely resolutions of national and international issues involving telecommunications standards and the development of operational guidelines. ATIS initiates and maintains open industry forums to address technical and operating issues affecting the nation's telecommunications facilities and services, and the development of innovative technologies. ATIS serves as an information resource to its members, its forum participants and other interested parties. It promotes industry progress and harmony with minimal regulatory or legislative intervention.

This government/industry group had been meeting for more than a year prior to its request for ATIS sponsorship. In order to continue the group's momentum, there was a period of transition to full ATIS sponsorship. The first meeting of the ECSP Committee under ATIS auspices occurred on September 1, 1993. The committee has adopted a set of Operating Principles, and selected Committee co-chairpersons; one from the industry and the other representing law enforcement.

Membership in the ECSP Committee is open to all providers of electronic communications services, as defined in Section 2510, Title 18 of the U.S. Code, U.S. law enforcement agencies that are empowered to perform lawfully authorized intercepts of communications, telecommunications equipment manufacturers, and others, such as trade associations, subject to ECSP Committee approval. Due to the sensitive nature of the information that is discussed at ECSP Committee meetings, attendance and access to ECSP Committee information is limited to ECSP Committee members and invited guests who have signed a nondisclosure agreement.

Industry membership presently includes all of the major local exchange carriers, (LECs), interexchange carriers (JC's), major equipment manufacturers such as AT&T, Northern Telecom and Siemens Stromberg Carlson, cellular service providers, and industry trade associations such as United States Telephone Association (USTA), and the Cellular Telecommunications Industry Association (CTIA). Law enforcement membership comes from many city, county, state and federal law enforcement organizations.

The Committee operates through Action Teams, which study specifically identified and designated issues. These issues focus on sophisticated communications technology, identified by the Committee, which impact on the ability of federal, state and local law enforcement agencies to conduct court-approved electronic surveillance. The Action Teams identify potential solutions, which are made available to the participants for voluntary implementation in their networks.

The efficacy of this kind of government-industry cooperation and coordination should not be discounted in determining how to legislatively address electronic surveillance issues in a timely and cost-efficient manner.

IV. HOW WIRELESS WIRETAPS WORK

In order to fully understand the issues involved in this debate, it is necessary to understand how a wireless system works to facilitate a lawful wiretap. As described previously, when a subscriber places a call from a mobile unit, the call comes to the MTSO. The MTSO, or switch, is a sophisticated computer that processes the call and routes it where it needs to go (Section II, *supra*). Each switch contains several "ports," as do most computers, which allow access to the programs and processes that take place internally and are essential to conducting maintenance. It is at this point, using an available port, that the call content and call detail information can be intercepted.

---

[3] 18 U.S.C. §2518(4).

While switches, usually in the major markets, have sufficient port capacity, a particular MTSO may need additional port capacity because of heavy wiretap demands in that market. Such additional port capacity can be added, within the limits of the physical surroundings of the switch. Typically, such capacity increase comes in banks of 24 ports which costs around $200,000 per bank with associated software.

When a wireless user roams, the tap occurs in the same way at the MTSO in the distant market. The IS–41 network, discussed above in Section II, alerts law enforcement that the suspect has moved and identifies the new location. With this information, a lawful warrant can be obtained from the proper court and the tap can be put on the MTSO at the new site. [It should be noted that this capability is switch-dependent and some in-service switches will need to be upgraded. The cost of such upgrades will vary depending on the type and quality of switch in service, but can be quite expensive.]

There are two types of information which law enforcement seeks through wiretaps. One is the information regarding the call, that is, the number dialed and other "call setup" information. The other information is the content of the call itself (the conversation or the data transmitted during the call).

Call setup information is the MTSO's resident internal data that is used to establish a link to the cellular subscriber. This information contains: (1) call destination (dialed digits); (2) identity of the location of the incoming call; (3) date, time, and duration of the call; and (4) first and/or last cell site used to deliver the call.

All cellular switches provide call setup information. The only issue is how quickly it is available. As a call is completed, the call detail information is stored in the switch's billing records data element and every 24 hours those records are transferred into a data base, at which time the call detail information can be withdrawn. Thus, any cellular system today can provide call detail in an average time of 12 hours. Recognizing law enforcement's desire for immediate call detail information, software has been developed which can pull the call detail immediately upon completion of the call. This capability has been developed without legislation and is now available on switches made by three of the four major switch manufacturers. The average cost for such capability is $50,000.

Dialed digits can be obtained pursuant to what is called a "pen register" warrant. However, pen register warrant authority does not grant law enforcement access to call content. Pursuant to a Title III warrant, law enforcement may obtain call content information on a real-time basis. In order to obtain call content information, law enforcement must simply access a port on the MTSO that processes the call.

V. PROPOSED LEGISLATION

The House and Senate Judiciary Committees and their professional staffs are to be congratulated for the substantial revisions that have been made to the original draft proposal put forth by the FBI entitled "The Digital Telephony and Communications Privacy Act of 1994". On the whole it is a much improved statement of the needs of law enforcement and of the obligations imposed upon the telecommunications industry to meet those needs. We would call your attention to several specific provisions of the legislation.

A. Cellular Fraud—Importantly, in addressing law enforcement's electronic surveillance needs, another criminal activity has been addressed in this revised legislation as well. We've all heard the stories of someone receiving a cellular bill for thousands of dollars for calls they did not place. Criminals are utilizing techniques such as "cloning" and "tumbling" electronic serial numbers ("ESN's") to obtain service fraudulently. Cellular companies are presently losing a million dollars a day to fraudulent tampering and alteration of the mobile telephone unit. The proliferation of the fraudulent use of wireless telephones through such techniques is not just a business dilemma, however. If law breakers can make one wireless phone impersonate another with impunity and without fear of punishment, then lawful wiretaps can be compromised since neither a wireless carrier's switch nor law enforcement will know right away which is the "real" number and user.

Today, fraudulent alteration of a wireless phone can be accomplished relatively easily. Each phone is originally programmed with a unique electronic serial number (ESN) at the time of manufacture. When a customer purchases the phone and subscribes to a particular carrier's service, a separate mobile identification number ("MIN") is programmed into the phone. This ESN/MIN combination becomes the wireless system's means of verifying the identity of the subscriber (it is this information, for instance, which is hauled over the 1541 network to allow tracing of a mobile phone to a foreign market). The ESN/MIN is transmitted continuously to a wireless carrier's switch while the subscriber's phone is in the "on" position. The switch verifies that the ESN/MIN combination is a legitimate account and then processes the call.

Utilizing scanner equipment and off-the-shelf software and hardware, a person desiring a cloned phone can capture the subscriber's ESN/MIN off the air and reprogram another phone with that same ESN/MIN combination. Often, the first time there is an awareness that the ESN/MIN has been cloned is when a subscriber reports to his carrier that a bill has been received with charges for calls to points around the country or world that the subscriber did not make. The carrier then must program the switch to discontinue processing calls from that ESN/MIN combination and the subscriber is given a new combination.

There are currently over 16 million subscribers using analog wireless phones and it will be many, many years, if ever, before all analog phones are phased out of service and all subscribers are converted to digital. While the introduction of digital technology may slow the pace of cloning temporarily, it can be expected that creative criminal elements and "phone hackers" will soon be able to alter these devices as well.

Altering or reprogramming a wireless phone's ESN or MIN can seriously impact the constitutional and statutory limitations of wiretap procedures as well. A suspect who is using a cloned phone is actually using a wireless communications system's electronic identification of another person without their consent. It is possible then that government will inadvertently intercept one person's private conversations when it thinks it is intercepting another.

In addition to such privacy concerns, the evidentiary ramifications are equally alarming. Because of the existence of cloning, law enforcement may not be able to guarantee that the content and call detail information it intercepts originates from the suspect who is the target of the wiretap. Thus, it can result in the government being unable to establish the requisite link between the tapped suspect and the intercepted call content/call detail needed to incriminate the suspect.

Even when it becomes apparent that a suspect is using a cloned phone and counter-measures are taken, such as giving the legitimate subscriber a new phone with a different ESN/MIN, there is nothing to prevent the target suspect from merely reprogramming his phone with yet another stolen ESN/MIN of another legitimate subscriber. In fact, today's wireless pirates have the ability to reprogram a phone every time a call is made.

The hardware and software necessary for such alterations are readily available and by themselves are not illegal to possess. The use of these unauthorized counterfeit phones is not clearly a crime either. Section 1029 of Title 18, entitled "Fraud and related activity in connection with access devices," enacted primarily to address credit card fraud, has been the only statutory provision available to the Secret Service and U.S. Attorneys to prosecute these acts. Some federal district courts, and recently the 10th Circuit Court of Appeals,[4] have determined that this statute does cover the possession of cloning equipment or the use of cloned phones even when it is clear from the facts that such possession and use are for fraudulent purposes.

This dilemma can only be remedied by Congressional initiative to clearly make such acts illegal, and then by a concerted effort from law enforcement to work with industry to curtail such activity and the proliferation of the paraphernalia utilized in association with such acts. The wireless industry is pleased to see that this revised legislation does contain such an initiative.

B. Capacity Determinations—The manner in which law enforcement makes a determination of its wiretap capacity must be a very cost-efficient mechanism to ensure that federal funds are not being unwisely or unnecessarily expended. An area where the legislation could be strengthened is the linkage between wiretap capacity and cost.

The amount of the bill presented to the taxpayers will be determined by the size of the wiretap capacity wish list developed by law enforcement. Human nature being what it is, one party will want it to be as large as possible while the other will seek just the opposite. As presently drafted, there is no mediation among these conflicts, save for a unilateral determination by the Attorney General.

We urge you to include in the capacity determination, a notice and comment rulemaking which affords the parties the opportunity to build a record.

---

[4] The 10th Circuit Court of Appeals recently ruled that Section 1029 does not apply to cellular "tumbling" fraud. *United States* v. *Brady*, No. 934085, slip op. at 13–14 (Dec. 21, 1993) ("Although Congress, without question, has the power to criminalize the use of or trafficking in cellular telephones altered to allow free riding on the cellular telephone system, even when such telephones do not access valid identifiable accounts, Congress did not do so when it enacted § 1029").

C. Roaming—The revised legislation addresses the concerns that the wireless industry expressed over the cost and complexity to add capability to retrieve content in a roaming environment. Wireless technology, fortunately, has the capacity to advise law enforcement when a target has traveled outside the home market, and to identify this roaming market in which the target may be using his or her cellular phone. This then, enables a tap to be put on the switch in the distant market.

One of the great improvements made in the legislation was a recognition of how this capability can be used effectively and at lower cost than previously proposed alternatives.

D. Cost Reimbursement—The revised legislation provides that the government reimburse industry service providers for the reasonable costs incurred in establishing the capabilities deemed necessary to ensure the ability to continue to conduct lawful electronic surveillance, as well as to reimburse costs incurred to expand capacity to meet the projected demands. It remains, however, an open question as to what will ultimately be the full extent of those costs. Until each carrier examines its system status in light of these legislated capability requirements, and until the capacity requirements of law enforcement agencies at the state and federal level have been quantified, and until price quotes are obtained from manufacturers and suppliers on the necessary changes and additions to these systems, an accurate projection of costs cannot be known.

We would urge the Congress to delay implementation or compliance dates until it has determined these cost elements. There is a Catch-22 in the offing if Congress does not first make such factual determinations. Carriers will be required to provide capacity and suffer penalties for the failure to do so—and the taxpayers will be required to fund the capacity without either party knowing the extent or nature or cost of that capacity. What this legislation could end up creating, therefore, is a requirement (and penalties) for the carriers and insufficient funding—simply because the capacity requirement was a wish list, not an optimal solution.

For instance, there are just over 1,100 cellular switches in operation covering 1,529 systems nation-wide. However, a review of the wiretap data reveal that of the 225 wiretaps executed on cellar systems, 50 percent were performed in only two states. 80 percent of the total were executed in only six states [see attachment A]. While the data doesn't reveal the cities in each state where the taps occurred, it is likely that only one major city in each state was the principal location.

This kind of information coupled with accurate cost data, can enable the Congress to make an informed decision as to whether or not it is a wise use of tax-payer dollars to require outlays for many wireless systems in the nation to meet the capability requirements, or whether it would be better to establish a method to prioritize necessary system upgrades in relation to wiretap demands over a longer period of time. This would avoid imposing unreasonable demands upon the federal treasury, and avoid the potential imposition of lengthy delays in the reimbursement of such costs to the telecommunications carriers, where unreimbursed outlays can have a substantial impact on operations, particularly for the smaller and newer carriers.

VI. CONCLUSION

The testimony presented today is intended to illustrate that the wireless telecommunications industry's history of supporting the lawful needs of the FBI and other law enforcement agencies around the country as regards surveillance requirements. It is the industry's intention to continue to work closely with law enforcement to maintain that compliance.

To the extent that the Congress deems this additional legislation necessary to fully ensure future capacity and capability of both industry and law enforcement, a careful and reasoned approach to the many issues and the costs attendant thereto is vital, with meaningful input from the affected industry and public interests that have appeared before the Committees.

Finally, there a major criminal activity which is addressed in this revised legislation by the Congress—the fraudulent cloning of wireless technology that impedes law enforcement, intrudes on consumer privacy and defrauds wireless service providers. We strongly endorse this measure and urge its adoption in full.

Thank you for the opportunity to appear today. I will be happy to respond to any questions that you may have.

ATTACHMENT A

Cellular Wiretaps Calendar Year 1993

Location	Federal	State	Total
New York	16	68	84
Florida	18	11	29
Texas	18	3	21
New Jersey	4	12	16
California	11	2	13
Michigan	13	0	13
Pennsylvania	2	6	8
Ohio	4	0	4
Illinois	3	0	3
Kentucky	3	0	3
Louisiana	3	0	3
Missouri	3	0	3
Nevada	3	0	3
Oregon	1	2	3
Arizona	2	0	2
Colorado	2	0	2
Connecticut	2	0	2
WDC	2	0	2
Maryland	0	2	2
Massachusetts	0	2	2
Minnesota	2	0	2
Nebraska	2	0	2
Arkansas	1	0	1
Indiana	1	0	1
Tennessee	1	0	1
Total	117	108	225

Total Wiretaps (all types) for 1993=976. Cellular wiretaps for 1993=225.
Less than ¼ of all wiretaps are cellular.
Source: Administrative Office of the United States Court Wiretap Report. For the period January 1, 1993 to December 21, 1993.

Representative EDWARDS. Thank you, Mr. Wheeler.

I am sure that you all can count on the Congress, both in the House and in the Senate, working closely in the years ahead as these problems develop. We are pretty resilient around here, especially where something as important as this is concerned, so I hope we can handle that in the future.

The last member of the panel is Jerry Berman, who for many years has worked both with the Senate committees and the House committees and has always been a trusted expert on privacy. Mr. Berman is Director of the Electronic Frontier Foundation.

Welcome, Mr. Berman.

STATEMENT OF JERRY BERMAN, DIRECTOR OF POLICY, ELECTRONIC FRONTIER FOUNDATION

Mr. BERMAN. Thank you, Chairman Edwards, and thank you, Chairman Leahy, for allowing me to testify today.

Like the other witnesses, I really want to commend both of you and your staffs and Senator Biden's staff and Ken Mendelson with Chairman Brooks for having really done an incredible job in transforming a bill which we saw as a potential privacy nightmare into a bill which is carefully crafted to protect privacy, not only as industry is required to meet and continue to deliver a wiretap capability subject to court authorization, but in recognizing that technology is a two-way street.

When technology hampers law enforcement, law enforcement makes a case that it requires legislation or redress. They have made that case. We might believe that it could have been done with a funding bill or some other vehicle, but we are beyond that. But I think that what you have crafted here is a bill that is very narrow in scope. It leaves out information services, the Internet, the manipulators of content on the information highway, which were included in the last bill, and that was a very troubling thing. They are not here.

You have set up an open standards process, allowed industry to make standards, allowed privacy interests to be taken into account in the design feature, and also allowed privacy advocates to intervene in this process if security interests are at stake.

I think that subject to resolving the cost issue, which I will come back to at the end of my statement, in the legislative process as we go forward, I think that if we are going to pass a digital telephony bill, this is the bill to pass.

I must also point out that the other side of the technology street is that when technology advances, privacy can also be impaired and undermined and eroded. This legislation, unlike previous drafts, as the FBI Director has pointed out, deals with some of those privacy problems that have been created by the evolving technology and which Senator Leahy's task force in 1991 identified and which the presence of a Digital Telephony bill gave us an opportunity to look at the other side of the issue.

I really want to point out that in addition to the changes that were made for cordless phones and so forth, that significant advances have been made here for privacy in the kind of electronic world we are going to be and increasingly living in.

This legislation requires that the FBI get a court order, based on reasonable suspicion and articulable facts, that in order to get the transactional information that is generated in electronic messages and E-mail messaging. In many ways, it looks like just addressing information which in other regimes is subject to a subpoena. Here, a court order is being imposed because of the recognition that the richness of these transactions, the fact that it really, on a minute-by-minute basis, can tell you who you are talking to, what you are doing, what you are interested in, it reveals content. So the committee and the Congress is recognizing, and the FBI is agreeing, that it deserves higher scrutiny, and that is an important protection that is in this bill.

It is also important that one of the requirements that the committee has imposed is a requirement not to design ongoing location features into the electronic technology for communications. We do not want to turn our cellular and radio-based communication systems into nationwide tracking systems for persons who may be of interest to law enforcement and who are not subject to a warrant.

It is important that the legislation also says that the additional information which is gained by pen registers, because it captures more digits than just that which reveal the telephone number, has to be stripped off and they have to move toward technology which strips it off, because more and more content is coming through the touch-tone phone over a pen register.

It is also important that this legislation says that carriers have no responsibility to decrypt any communications, so that people using encryption technology for their privacy, you have to move those communications across this network, which is very important and, of course, is the subject of another ongoing debate which Senator Leahy has been working on and which I am sure we will return to again next year.

As the Director points out, it is also important that this technology can be designed so that you can have an on/off switch at the central office that will allow the FBI to turn on taps from a remote site. This legislation says they cannot do that.

I have already pointed out that there are privacy protections built into the requirements process, so as a whole package, I think that these are significant advances for privacy and make the whole package a balanced approach, and if legislation is going to happen, it ought to be this vehicle. We are hoping to work with you to ensure that it stays together and is improved and perfected, and I think we can do maybe more clarifying language on the reasonableness test. I don't want to bother you with a minimization issue that we have, but we will come back to that in the discussion process.

I want to come back to the cost issue. There is a letter which the Electronic Frontier Foundation as an advocacy organization has signed along with long-distance carriers and the telephone industry to both of you, to the chairs of the committee and to the committee, saying that we need to resolve this cost issue.

The estimates of $500 million on the one hand and several billion dollars on the other hand from the telephone industry, with GAO saying it is a complicated issue, we think needs to be nailed down, not only for us to know where we are diverting dollars from one priority, like law enforcement, or taking from innovation or expansion of the information highway, but it is a significant privacy issue.

The whole point of this bill turns on there being a compliance process which is reasonable and we need to have a cost on the top of the table and they need to be capped in some way, both to force the FBI and law enforcement to do what they want to do, which is set priorities, but also let industry know that they are going to be paid.

If those issues are not addressed, there is the possibility of skimping on costs which could present privacy problems, or on the other hand, building more capacity into the network because the Government doesn't have to pay for it and they ask for more than they may need because they want to take care of law enforcement. There, we have more capacity than we need and that presents a privacy threat at that level.

So I think that that is an issue which we did not resolve in the negotiating process and I think it is important to nail down in the legislation.

Again, I appreciate the efforts that you have gone through. We have been working with you in a spirit of cooperation, along with the whole coalition. We hope to continue as the process goes forward. Thank you very much.

[Mr. Berman submitted the following:]

PREPARED STATEMENT OF JERRY J. BERMAN ON BEHALF OF THE ELECTRONIC FRONTIER FOUNDATION

Chairman Leahy, Chairman Edwards and Members of both subcommittees: I want to thank you for the opportunity to testify today on your new version of the

Digital Telephony bill (H.R. 4922, S. 2375). The Electronic Frontier Foundation (EFF) is a public interest membership organization dedicated to achieving the democratic potential of new communications and computer technology and works to protect civil liberties in new digital environments. EFF also coordinates the Digital Privacy and Security Working Group (DPSWG), a coalition of more than 50 computer, communications, and public interest organizations and associations working on communications privacy issues. am testifying today, however, only on behalf of EFF.

Since 1992, the Electronic Frontier Foundation has opposed a series of FBI Digital Telephony proposals, each of which would have forced communications companies to install wiretap capability into every communications network. However, earlier this year, when it became apparent that some version of the bill would pass the Congress, the Subcommittees asked EFF along with computer and communications industry groups to participate in a process that would yield a narrow bill that both met law enforcement needs and had strong privacy protections. The result of that process is the bill we have before us today. EFF remains deeply troubled by the prospect of the federal government forcing communications networks to be made 'wiretap ready,' but we believe that this legislation is substantially less intrusive that the original FBI proposals.

The bill is significantly more narrow than the original proposals in that it exclude a number of electronic communications service providers—including online information services, Internet access providers, electronic bulletin board systems, PBX's, and private networks—from any compliance obligation. In particular, the Leahy/Edwards version contains a number of important changes from earlier proposals, including:

- A narrow Scope,
- Open standard-setting process with public right of intervention,
- Technical requirements standards developed by industry instead of the Attorney General,
- Right to deploy untappable services.

In my testimony today, however, I would like to review what I believe to be the most important privacy protections of this bill, and to discuss the areas which EFF still believes require more attention before a bill is passed.

A. NEW PRIVACY PROTECTIONS

The Digital Telephony legislation before us includes significant recognition that new communication technologies, and new patterns of technology use, require new privacy protections. Thanks to the work of Senator Leahy and Representative Edwards and Senator Biden, the bill contains a number of significant privacy advances, including enhanced protection for the detailed transactional information records generated by on line information services, email systems, and the Internet.

1. Expanded protection for transactional records sought by law enforcement

Chief among these new protections is an enhanced protection for transactional records from indiscriminate law enforcement access. Many online communication and information systems create detailed records of users' communication activities as well as lists of the information that they have accessed. Provisions in the bill recognize that this transactional information created by new digital communications systems is extremely sensitive and deserves a high degree of protection from casual law enforcement access which is currently possible without any independent judicial supervision.

EFF commends Senator Leahy, Representative Edwards, and Senator Biden for declaring that law enforcement access to transactional records in online communication systems (everything from the Internet to AOL to hobbyist BBS's) threatens privacy rights. Privacy interests are implicated because:

- The records are personally identifiable,
- They reveal the content of people's communications, and,
- The compilation of such records makes it easy for law enforcement to create a detailed picture of people's lives on line.

Based on this recognition, the draft bill contains the following provisions:

- Court order required for access to transactional records instead of mere subpoena

In order to gain access to transactional records, such as a list of to whom a subject sent email, which online discussion group one subscribes to, or which movies you request on a pay-per view channel, law enforcement will have to prove to a court, by the showing of "specific and articulable facts" that the records requested are relevant to an ongoing criminal investigation. This means that the government may not request volumes of transactional records merely to see what it can find through traffic analysis. Rather, law enforcement will have to prove to a court that it has reason to believe that it will find specific information relevant to an ongoing criminal investigation in the records it requested.

With these provisions, we have achieved for all online systems, a significantly greater level of protection than exists today for records such as email logs, and greater protection than currently exists for telephone toll records. The lists of telephone calls that are kept by local and long distance phone companies are available to law enforcement without any judicial intervention at all. Law enforcement gains access to hundreds of thousands of such telephone records each year, without a warrant and without even notice to the citizens involved. Court order protection will make it much more difficult for law enforcement to go on "fishing expeditions" through online transactional records, hoping to find evidence of a crime by accident. We have also submitted a detailed memorandum on the importance of protection and would ask that this document be included in the record of these proceedings along with this testimony.

- Standard of proof much greater than for telephone toll records, but below that for content

The most important change that these new provisions offer is that law enforcement will: (a) have to convince a judge that there is reason to look at a particular set of records, and; (b) have to expend the time and energy necessary to have a United States Attorney or District Attorney actually present a case before a court. However, the burden or proof to be met by the government in such a proceeding is lower than required for access to the content of a communication.

2. New protection for location-specific Information available In cellular, PCS and other advanced networks

Much of the electronic surveillance conducted by law enforcement today involves gathering telephone dialing information through a device known as a pen register. Authority to attach pen registers is obtained merely by asserting that the information would be relevant to a criminal investigation. Under current law, courts must approve pen register requests without any substantive review of the basis for law enforcement's request. This legislation offers significant new limits on the use of pen register data.

Under this bill, when law enforcement seeks pen register information from a telecommunications carrier, the carrier is forbidden to deliver to law enforcement any information which would disclose the location or movement of the calling or called party. Cellular phone networks, PCS systems, and so-called "follow-me" services all store location information in their networks. This new limitation is a major safeguard which will prevent law enforcement from casually using mobile and intelligent communications services as nation-wide tracking systems.

3. New limitations on "pen register" authority

Contemporary uses of pen registers also involve substantial privacy invasion, even aside from location information. Currently, law enforcement is able to use pen registers to capture not only the telephone number dialed, but also any other touchtone digits dialed which reflect the user's interaction with an automated information service on the other end of the line, such as an automatic banking system or a voicemail password. If this bill is enacted, law enforcement would be required to use "technology reasonably available" to limit pen registers to the collection of calling number information only. We are aware that new pen register devices are now on the market which automatically screen out all dialed digits except for the actual telephone numbers. Just as this bill would require telecommunications carriers to deploy technology which facilitates taps, we believe that law enforcement should be required to deploy technology which shields users communications from unauthorized invasion.

4. Bill does not preclude use of encryption

Unlike previous Digital Telephony proposals, this bill places no obligation on telecommunication carriers to decipher encrypted messages, unless the carrier actually holds the key to the message as well.

5. Automated remote monitoring precluded

Law enforcement is specifically precluded from having automated, remote surveillance capability. Any court-ordered electronic surveillance must be initiated by an employee of the telecommunications carrier, upon request by law enforcement.

Maintaining operational separation between law enforcement agents and communication networks is an important privacy safeguard.

6. Privacy considerations essential to development of new technology

One of the requirements that telecommunications carriers must meet to be in compliance with the Act is that the wiretap access methods adopted must protect the privacy and security of each user's communication. If this requirement is not met, anyone may petition the FCC to have the wiretap access service be modified so that network security is maintained. This requirement, just like those designed to serve law enforcement's needs, must be carefully implemented and monitored so that, the technology used to conduct wiretaps cannot also jeopardize the security of the network as a whole. If network-wide security problems arise because of wiretapping standards, then the standards should be overturned.

B. DIGITAL TELEPHONY REQUIREMENTS NARROWED AND PUBLIC PROCESS BROADENED

In addition to the privacy protections added to this bill, we also note that the surveillance requirements are not as far-reaching as the original FBI version. A number of procedural safeguards are added which seek to minimize the threatens to privacy, security, and innovation. Though the underlying premise of the Act is still cause for concern, these new limitations deserve attention:

1. Narrow scope

The bill explicitly excludes Internet providers, email systems, BBS's, and other online services. Unlike the bills previously proposed by the FBI, this bill is limited to local and long distance telephone companies, cellular and PCS providers, and other common carriers.

2. Open process with public right of intervention

The public will have access to information about the implementation of the Act, including open access to all standards adopted in compliance with the Act, the details of how much wiretap capacity the government demands, and a detailed accounting of all federal money paid to carriers for modifications to their networks. Privacy groups, industry interests, and anyone else has a statutory right under this bill to challenge implementation steps taken by law enforcement if they threaten privacy or impede technology advancement.

3. Technical requirements standards developed by industry instead of the Attorney General

All surveillance requirements are to be implemented according to standards developed by industry groups. The government is specifically precluded from forcing any particular technical standard, and all requirements are qualified by notions of economic and technical reasonableness.

4. Right to deploy untappable services

Unlike the original FBI proposal, this bill recognizes that there may be services which are untappable, even with Herculean effort to accommodate surveillance needs. We understand that the bill intends to allow untappable services to be deployed if redesign is not economically or technically feasible. These provisions, however, should be clarified.

C. PROVISIONS THAT REQUIRE FURTHER AMENDMENT BEFORE FINAL PASSAGE

EFF plans to work on the following issues in the bill as the legislative process continues:

1. Strengthened public process

In the first four years of the bill's implementation, most of the requests that law enforcement makes to carriers are required to be recorded in the public record. However, additional demands for compliance after that time are only required to be made by written notice to the carrier. All compliance requirements, whether initial requests or subsequent modification, must be recorded in the Federal Register, to allow for public scrutiny.

2. Linkage of cost to compliance requirements—the FBI gets what it pays for and no more

The bill authorizes, but does not appropriate, $500 million to be spent by the government in reimbursing telecommunications carriers for bringing their networks into compliance with the bill. The FBI maintains that this is enough money to cover all reasonable expenses. The industry, however, has consistently maintained that the costs are five to ten times higher. Given the FBI's confidence in their cost estimate, we believe that telecommunications carriers should only be required to comply to the extent that they have been reimbursed.

The bill as introduced wisely includes detailed reporting requirements for all reimbursements to carriers for retrofits during the first four years. Not only is this fiscally responsible, but also it allows those concerned about privacy and civil liberties to monitor the deployment of surveillance technology. From a civil-liberties perspective, this is a crucial safeguard.

However, after four years, reimbursement will be limited to costs incurred for adding capacity only, not including surveillance capability in new services. This defeats the purpose of providing public scrutiny of the government's surveillance expenditures. We are concerned that failure to limit the bill's requirements to actual reimbursements will cause deployment of unnecessary surveillance capability around the country that would be a threat to privacy and civil liberties.

3. Ensure right to deploy untappable services

The enforcement provisions of the bill suggest, but do not state explicitly, that services which are untappable may be deployed. The bill should be state directly that if it is technically and economically unreasonable to make a service tappable, then it may be deployed, without interference by a court.

4. Clarify definition of call identifying information

The definition of call identifying information in the bill is too broad. Whether intentionally or not, the term now covers network signaling information of networks which are beyond the scope of the bill. As drafted the definition would appear to require telecommunications carriers to deliver not only the signaling information generated by their own services, but also the signaling information generated by information services and electronic communication services that travel over the facilities of the telecommunication carrier. In many cases this may be technically impractical. Moreover, it is contrary to the policy adopted by the bill to maintain a narrow scope.

5. Review of minimization requirements in view of commingled communications

The bill implicitly contemplates that law enforcement, in some cases, will intercept large bundles of communications, some of which are from subscribers who are not subject of wiretap orders. For example, when tapping a single individual whose calls are handled by a PBX, law enforcement may sweep in calls of other individuals as well. Currently the Constitution and Title III requires "minimization" procedures in all wiretaps, to minimize the intrusion on the privacy of conversations not covered by a court's wiretap order. In the world of 1968, when the original Wiretap Act was passed, most subscribers telecommunications facilities carried single conversations on single lines. But today, many conversations are co-mingled on one broadband communications facility. In order to ensure that constitutionally-mandated minimization is maintained, the bill should recognize that stronger minimization procedures may be required.

D. CONCLUSION

In closing, I would like to thank both subcommittees, as well as others who have worked so hard on this legislation. The Electronic Frontier Foundation looks forward to working with all of you as the bill moves through the legislative process.

ELECTRONIC FRONTIER FOUNDATION, INC.,
Washington, DC, August 11, 1994.

Chairman PATRICK LEAHY,
Subcommittee on Law and Technology,
Senate Judiciary Committee, Washington, DC.

Chairman DON EDWARDS,
Subcommittee on Civil and Constitutional Rights,
House Judiciary Committee, Washington, DC.

DEAR CHAIRMEN LEAHY AND EDWARDS, All of us in the Digital Privacy and Security Working Group wish to thank you and your staffs for the extraordinary leadership that you have shown in the process of crafting Digital Telephony legislation. Over the last few months, the bill has been transformed from a proposal that was wholly one-sided to one that is considerably more reasonable. However, one of the most significant outstanding issues is the calculation of the overall costs that will be incurred in complying with the bill, and the appropriate policy for determining who should pay for this compliance.

Among the major improvements of the Leahy/Edwards bill over the original Bush Administration proposals is that the federal government has taken responsibility to pay for at least the initial retrofit costs incurred in complying with the requirements of the Act. However, the magnitude of these costs remains a source of significant dispute.

- No reliable costs estimates—FBI estimates are too low and based on faulty assumptions

The legislation as introduced authorizes $500 million over a four year period to pay for redesign of services that the FBI believes are currently causing problems. Yet Director Freeh himself testified before your joint hearing in March that costs could run to $1.5 billion. Industry estimates put compliance costs at $2 billion to $3 billion dollars.

While we are awaiting the report from the General Accounting Office on the cost issue, we already have further reason to doubt the FBI's cost estimates. For example, we know that the FBI estimates fail to account for new competitors that are already entering the local telecommunications market in competition with the local exchange carriers. Cable companies, for example, are already deploying technology which will allow them to offer local telephone services as a complete replacement for the service now provided by the local telephone companies. Yet, the FBI has failed to account for the costs that these new firms may incur under the Act as proposed.

We hope that you will use the hearing process now beginning to explore on the public record the true costs of the FBI's proposal. That current costs estimates diverge by factor of at least six causes us great concern.

- Failure to cover "out year" costs assumes static technology and will stifle Innovation and competition

The structure of the current bill presumes that capability compliance costs will be de minimis after the first four years of retrofits are completed. We disagree with this presumption. Four to six years may or may not be enough time to modify current telecommunication services to meet law enforcement needs. Yet new services are being deployed every day in the telecommunications market. In some cases, accomplishing surveillance needs may be relatively simple during the design process. But in other cases, substantial effort and expense will be required. If the bill is enacted with its current cost treatment, it will certainly discourage the deployment of new communications services once reimbursement is no longer available.

The four-year cap on reimbursement also ignores the fact that many new competitors are planning to enter the telecommunications market. No matter how this legislation is ultimately written, the technology needed to comply will be packaged by telecommunications equipment manufacturers as individual features. Each feature carries a cost to the manufacturer and a price to the telecommunications carriers that purchase them. New entrants into the communications marketplace would have to purchase these features. If they enter after the four-year reimbursement period expires, then they would have to bear the cost on their own, despite the fact that the incumbents in the market may have been reimbursed for that same cost by the federal government. As such, the current reimbursement structure runs counter to the overall United States communications policy, which seeks to promote competition in the local telecommunications market.

- Privacy and civil liberties will be victim without firm spending cap

The Leahy/Edwards bill as introduced wisely includes detailed reporting requirements for all reimbursements to carriers for retrofits during the first four years. Not only is this fiscally responsible, but also it allows those concerned about privacy and civil liberties to monitor the deployment of surveillance technology. From a civil-liberties perspective, this is a crucial safeguard.

After four years however, reimbursement will be limited to costs incurred for adding capacity only, not including surveillance capability in new services. This defeats the purpose of providing public scrutiny of the government's surveillance expenditures. We are concerned that failure to limit the bill's requirements to actual reimbursements will cause deployment of unnecessary surveillance capability around the country that would be a threat to privacy and civil liberties.

- Proposal Expand current bill's provisions which link compliance obligations to reimbursements

In recognition of the fact that current cost estimates are inconclusive, and that the long-term cost of compliance is virtually impossible to estimate, we recommend that existing provisions in the bill that link compliance obligations to reimbursement be expanded. In the first four years, telecommunications carriers should be liable for compliance only to the extent that they have been reimbursed by law enforcement for the costs of retrofitting existing services. Such a provision would actually allow the Attorney General to allocate limited resources in the most efficient way possible and would eliminate pressure from carriers to be reimbursed for retrofits which law enforcement does not consider critical.

Data supplied by the Department of Justice shows that the bulk of wiretaps occur in a very few areas of the country and only in the context of certain services. For example, in 1993 there were 225 taps on cellular phone services, but fully 50 percent of those occurred in only two states, New York and Florida. (Similar patterns exist for wireline taps.) It would make sense, then, to target appropriated money to those areas where the need for retrofitting is great. However, since all cellular and wireline networks around the country are required to comply with the bill, they may request reimbursement from the Attorney General. Linking liability to reimbursement would give law enforcement the leeway to allocate its resources in the most sensible, efficient manner possible, and eliminate the need to pay for retrofits in areas, or for services, where the costs dramatically outweigh the benefits.

Following the four-year cutoff, existing telecommunications carriers as well as new entrants face substantial compliance costs, especially where new services are not easy to shape to law enforcement's requirements. Thus, there should be a mechanism for securing reimbursement.

If, after four years, costs are truly de minimis, then the expenses born by the taxpayer will be minimal. If, however, costs are substantial, the burden of compliance cannot be expected to be absorbed by private companies. The same linkage between reimbursement and compliance in the first four years should be applied to capability requirements in later years. This would protect American consumers from unreasonable demands by the government to pass surveillance costs through to the public sector and avoid public scrutiny.

We thank you for consideration of this matter, and look forward to working with you and your staffs toward a solution to this very important unresolved issue.

Sincerely,

AT&T,

CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION,

COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION,

COMPUTER AND BUSINESS EQUIPMENT MANUFACTURERS ASSOCIATION,

ELECTRONIC FRONTIER FOUNDATION,

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS—UNITED STATES ACTIVITIES,

MCCAW CELLULAR COMMUNICATIONS,

MCI COMMUNICATIONS CORPORATION,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION,

UNITED STATES TELEPHONE ASSOCIATION.

Expanded Protection for Online Transactional Information

Electronic Frontier Foundation, Inc.
1001 G Street, NW
Suite 950 East
Washington, DC 20001

Phone: (202)347-5400
Fax: (202)393-5509
Internet: eff@eff.org

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.... Can it be that the Constitution affords no protection against such invasions of individual security?[1]

I. Overview

A. Spirit of ECPA calls for expanded protection for network transactional information

In the eight years since the enactment of ECPA, society's patterns of using electronic communication technology have changed dramatically. Over twenty million people now have electronic mail addresses, numerous business, nonprofit and political groups conduct work over the Internet, and "cyberspace" has become a household world. Indeed, it is now commonplace to speak about "life online." Records of all of these activities -- who sends a message to whom, where a given communications device is located, which political party one contacts for information, and which online discussion group or virtual community one associates with -- are available both in real time and in stored form as part of the transactional information generated by advanced computer and communications networks. With increasing use of telecommunications, this transactional information reveals almost as much about our private lives as would be learned if someone literally followed us around on the street, watching our every move.

As the ECPA drafters recognized, "the law must advance with the technology to ensure the continued vitality of the Fourth Amendment."[2] Under current law, much of this transactional information may be available to law enforcement merely by subpoena which recites that the requested information is "relevant to an ongoing investigation."[3] In response to dramatic changes in the way that people use electronic communication services, ECPA should be revised to reflect the increasingly sensitive nature of network transactional information

---

[1] Olmstead v. United States, 277 U.S. 438, 467 (1928) (Brandeis, J., dissenting) (cited in ECPA Senate Report).

[2] ECPA Senate Report, p.5

[3] 18 USC 2703(d). As will be discussed below, the statutory distinction between contents and records is unclear, so that current scope of law enforcement access is not a matter of settled law.

B. Proposal to protect network transactional information that is personally identifiable or that reveals the contents of the communication

As this memorandum will demonstrate, the scope and depth of personal, sensitive information available through network transactional records has increased dramatically since the 1986 law was passed. Thus, EFF believes that the requirements for law enforcement access to certain categories of transactional records should be increased from a mere subpoena, which can be issued without independent judicial scrutiny, to a court order, which would only be issued upon a finding by a detached and neutral magistrate. All transactional records which:

- contain personally identifiable information related to an electronic communications, or
- reveal the content of the electronic communication

should be accessible to law enforcement only with a court order.

II. Online transactional information contains extensive personally identifiable information and thus deserves greater protection than telephone toll records

A. Personally identifiable information in online transactional records

The bulk of email addresses in use today are unique to an individual user. Either the address reveals on its face the identity of the user, or a simple command can be issued to translate the address into the owner's name.

Email addresses are personally identifiable

jberman@eff.org belongs to Jerry Berman
whitfield.diffie@eng.sun.com belongs to Whitfield Diffie

Therefore, unlike telephone toll records, a transaction indicating that a message is sent to or received from a particular email address is almost always a definitive record of a communication by an identifiable person. [For a detailed description of email transactional records, see Appendix A] Whereas, toll records record only the fact that a given telephone instrument connects an another instrument, a record of an email sent or received will establish the identity of the communicating party with some certainty. Ownership of a telephone instruments may be well-established, but without access to the content of the telephone communication, there is no proof that any individual was actually using the phone coincident with a communication recorded in toll records. In practice, courts also agree that toll records fall short of disclosing identity of the calling parties.[4]

Some early email systems tied the email address to a particular computer or terminal, just as a telephone number is tied to a given telephone instrument. But today, someone who owns an email address can use it from virtually any computer in the world. Moreover, no one else can easily use another person's email address, since the ability to send and receive mail with an address is generally controlled by password or other security device. While it is, in some cases, possible to use someone else's email address, this practice will increasingly be considered a fraud on the receiver of the message and a theft of service from the owner of the email account. By contrast, no fraud is required to use someone else's telephone number, unless one fails to pay the charges associated with the call.

B. Transactional records reveal location of sender and recipient

Transactional information in new mobile communications services such as cellular network and Personal Communications Services (PCS) provide law enforcement with information about the location and travel of users. These services are designed in order to deliver calls and other communications to the subscriber, no matter where in the country he or she is. As a side effect of this feature, the network generates trails of transactional information that pinpoint the users location at any time that the user has the device turned on. For example, when a cellular phone is set to "roam" from one territory to another, it signals the network each time it crosses into a new service area, so that calls can be delivered to that phone and so that proper billing connections are established.

Furthermore, transactional records from mobile communications services will also reveal the movement of an individual from place to place, in real time. As the target moves from one cell or service area to another, an electronic trace of the fact that a given geographical boundary line is crossed will be created. If law enforcement has access to such traces, it will be possible to determine not only the targets location, but also his or her direction of movement.

Such location specific information goes far beyond simple calling and called number information contemplated by Congress when it authorized access to transactional information without a warrant or other judicial scrutiny. Where a probable cause warrant has been issued, we do not contest law enforcement's right have access to such information, where technically feasible. However, we believe that it is contrary to the Fourth Amendment and to the policy framework established in the 1968 Act and ECPA, to allow access to this increasingly rich source of information based on subpoena authority alone.

---

[4] In United States v. Anderson (542 F.2d 428, 1976), the 7th Circuit found that "toll records could not be relied on to show the contents of calls nor the parties thereto; ... identification of places called ... did not reveal the identity of the recipient or the nature of the call..."

C. Online transactional records deserve a greater degree of protection than telephone toll records

In contrast to telephone toll records, online transactional information may reveal the identity of the communicating parties, and even the precise location of the communicators. These attributes distinguish online transactional records from traditional telephone toll records and other records generally available to law enforcement under subpoena power.

III. Content of communication revealed by online transactional information

In many instances, addressing information from online systems will reveal the content or subject of the electronic communication. As in the example below, messages are often directed to, or received from discussion groups on particular topics.

	EMAIL MESSAGE
FROM:	djw@eff.org (Danny Weitzner)
TO:	eff-crypto@eff.org,whitfield.diffie@sun.eng.com
RE:	crypto policy update
DATE:	July 29, 1994, 08:15:48
This week significant progress was made on the Clipper front, but slide continues on export control liberalization...	

This message would be sent to everyone who is a participant in this particular group. Discussion groups (such as eff-crypto) are similar to telephone conference calls, except that they may last for days, weeks, or years. [See Appendix A for discussion of online transactional records logs which reveal such information.]

Here again, email address records are dramatically more revealing than analogous telephone toll records. Telephone toll records might reveal the fact that the user of a particular telephone was connected to a conference call service, but would not indicate the subject of that conference. In the email example, above, the subject of the conference is embedded into the address line, along with other individual addressed. Furthermore, since the conference name is indistinguishable from an individual email address, there is no way to segregate such information out of the transactional record stream.

B. Freedom of association and assembly implicated by disclosure of personally identifiable information

Not only does the transactional log of such a discussion group reveal the contents of the discussion, but also, the names of the parties to the discussion are disclosed in the logs. This as an excerpt from an actual email log which records the progress of the above from the sender to all of the members of the online discussion group.

```
01 7/29 08:15:48 IIA12559: from=<djw@eff.org>, msgid=<199407291215.IIA12559@eff.org>
02 7/29 08:15:49 IIA12559: to="|/usr/local/etc/cryptoarchiver" stat=Sent
03 7/29 08:15:50 IIA12559: to="|/usr/local/etc/dmail2list eff-crypto eff-crypto [illegible]
04 7/29 08:15:51 IIA12565: from=owner-eff-crypto, msgid=<199407291215.IIA12559@eff.org>
05 7/29 08:15:51 IIA12565: to=gnu@toad.com (John Gilmore), delay=00:00:01, stat=queued
06 7/29 08:15:51 IIA12565: to=mkapor@kei.com (Mitchell Kapor), delay=00:00:01, stat=queued
07 7/29 08:15:51 IIA12565: to=jberman@eff.org (Jerry Berman), delay=00:00:01, stat=queued
08 7/29 08:15:52 IIA12565: to=jseiger@eff.org (Jonah Seiger), delay=00:00:01, stat=queued
09 7/29 08:15:51 IIA12565: to=djw@eff.org (Danny Weitzner), delay=00:00:01, stat=queued
```

First, line 1 of the log reveals that a message was sent to the eff-crypto discussion group. Then, lines 5 through 9 reveal the identity of all of the recipients of that message, in other words, all of the participants in this particular group.

For those who associate and assemble online, these email logs are equivalent to membership lists deserving of constitutional privacy protection. Inasmuch as online transactional records reveal the identity of the parties who are engaged in the discussion, fundamental constitutional rights such as freedom of association and freedom of assembly are implicated by any disclosure to the government. Since NAACP v. Alabama ex rel. Patterson, 357 US 449 (1958), courts have agreed that threats to privacy of association constitute impermissible intrusion on First Amendment freedom of association and freedom of assembly. The NAACP case involved a challenge to a government action which would have compelled the NAACP to disclose its membership list to the State of Alabama. The Supreme Court found that:

> Inviolability of privacy in group association may, in many circumstances, be indispensable to preservation of freedom of association. Id. at 462.

Inasmuch as online transactional records reveal such group association, they should be given a high level of protection from government intrusion. The transactional records of online conferences discussed above and is shown in Appendix A, clearly reveal association with particular groups.

IV. Quantity, Detail, and Ease of Analysis of transactional records require expanded protection

With the passage of ECPA , electronic mail messages were given the same degree of privacy protection as first class mail. Notwithstanding the analogy drawn in 1986, there are significant differences between email addressing logs and information which may be obtained under a mail cover.

A. Transactional logs of email contain significantly more Information than available from a mail cover

- **Automatic email transaction trail**

Email systems create detailed transaction logs as a matter of course, whereas the postal service only keeps address logs if specifically required to do so by valid legal process. Thus, in the case of email surveillance, law enforcement may decide after the fact of a particular transmission, to seek access to transactional records.

- **Automatic attachment of return address information**

When using US Postal Service mail, the addition of a return address which identifies the sender is entirely optional and requires an affirmative step by the sender. In contrast, most email systems automatically append a return address to each electronic mail message, thus guarantying that anyone who examines the email log, will be able to identify both the sender and recipient.

- **Email co-mingles functions traditionally accomplished with voice, fax, paper mail, and even face-to-face communications**

Email communication is often a substitute for many other forms of communications. An email message can replace a fax, a voice telephone call, a short note sent through the US mail, and even face-to-face communication. Therefore access to logs of such communication is vastly more revealing than a log of any other single form of communication. Courts have recognized an increased privacy interest in co-mingled information as compared to the same information in disaggregated form.

B. Increased privacy interest in compilations

The volume and detailed nature of email transactions raise much more serious privacy concerns than do either toll records or mail cover logs. The Supreme Court and the US Congress have recognized that computerized compilations of information raise unique privacy concerns. Beginning with the Privacy Act of 1974, Congress has acknowledged that "computerized data banks ... present issues considerably more difficult than, and certainly very different from, a case involving the source records themselves."[5] Later, in Whalen v. Roe, the Supreme Court found that "[t]he central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information."[6] And finally, in US Department of Justice v. Reporter's Committee, the Court found that a "strong privacy interest inheres in the nondisclosure of compiled computerized information...."[7] It is precisely the great volume of and easy access to transactional information which raises an increased privacy interest in these records.

---

[5] H.R. Rep. No. 1416, 93d Cong., 2d Sess. 3, 6-9 (1974) Legislative history of the Privacy Act of 1974.

[6] 429 U.S. 589, 607 (1977) (Brennan, J., concurring)

[7] 489 U.S. 749, 766 (1989)

V. Extend the spirit of ECPA to cyberspace: Need to update ECPA protections for transactional information in the changing digital world

The guiding principle of ECPA was that new privacy protection should be extended to electronic communications, so that users of new communications technology would have confidence that their communications were free from unwarranted private or government intrusion. With the qualitative shift in communications activity that has occurred over the last decade, it is time to extend greater protection to the transactional information that records people activities online.

A. Gaps left by 1986 law -- Unclear definition of transactional records

The main focus of ECPA was to offer clear privacy protection for the contents of electronic communication despite the fact that the communication is handed over to a third party, namely the electronic communication service provider.[8] However, little consideration was given at the time to the proper treatment of transactional records. The records are mentioned in the statute, but not given any definition. The committee report from the Senate does offer brief discussion of the nature of these records, but focuses primarily on customer lists and telephone toll records.[9] The House report recognizes that electronic communications services create records that do not conform to legal categories for older technologies:

> The newer technologies such as electronic mail and remote computing services maintain a type of records which do not neatly fit within the legal categories which exist for older technologies.[10]

---

[8] "A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law.... But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of computer technology. This is so even though American citizens and businesses are using these forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services." ECPA Senate report, p5.

[9] "Subsection (c) provides for access to records or other information pertaining to a subscriber to or customer of an electronic communications or remote computing service, not including the contents of electronic communications. This section permits the provider of the service to divulge, in the normal course of business, such information as customer lists and payments to anyone except a Government agency. It should be noted that the information involved is information about the customer's use of the service not the contents of the customer's communication." ECPA Senate Report, p. 38

[10] House Report, p. 26

However, nowhere in either committee report is the issue of access to email transactional records discussed for the purposes of establishing the appropriate standard for government access.

B. Extension of protection is consistent with the spirit of ECPA and the expressed intent of the drafters

In the spirit of ECPA, we should recognize that it is again time to extend privacy protection to the personally identifiable transactional information that is, in may cases, indistinguishable from content.[11] The drafters did not intend that electronic communication service providers should not disclose "profiles" of users that were related to the contents of the communication.[12] Furthermore, discussions of transactional records was limited at the time to telephone toll records and other customer account billing and demographic information.[13]

VI. Conclusion

This memo has shown that

- transactional records now reveal the content of communication,
- these records contain personally identifiable information,
- disclosure of such records implicate fundamental privacy and free association rights,
- current law is unclear as to the definition of such records, and,
- increased protection for transactional records is consistent with the spirit of the 1968 Act and the 1986 Act.

Therefore Congress should amend the stored communications section of ECPA (Sec 2703) to provide a higher level of protection for sensitive transactional records. The amendments would leave intact law enforcement's current authority regarding telephone toll records and basic billing information such as subscriber billing address and service arrangements. These changes to current law are necessary to provide assurances to users of new communication technology that their private activities in the online world are free from unwarranted interference.

For more information, please contact the Electronic Frontier Foundation:

Jerry Berman, Executive Director <jberman@eff.org>
Daniel J. Weitzner, Deputy Policy Director <djw@eff.org>

---

[11] Curiously, the original language in Title III, before it was amended by ECPA, provided that the "contents" of a communication included the "identity of the parties to such communication or the existence, substance, purport, or meaning of the communication." Thus, in 1968, telephone toll records were accessible under a lower standard precisely because they did not reveal the identity of communicating parties or the existence of the communication. Any transactional information which reveals the identity of the parties, or the content of the communication, should therefore be accessible to law enforcement only with a court order.

[12] ECPA House Report, p.64

[13] "The type of records involved are billing records and telephone toll records (including record of long distance numbers and message unit information." ECPA House Report, p. 69.

Appendix A

Telephone Toll Records and Electronic Mail Logs

The most significant difference between a telephone toll record and an electronic mail log is that electronic mail addresses are unique to individual users. Unlike a telephone number, which corresponds only to a specific location (such as a home or business address), most electronic mail addresses are linked by a secret and unique password[14] to an individual regardless of physical location. Thus, while a record indicating that a certain telephone number was dialed from another telephone number indicates that a transaction occured, an electronic mail record indicates that a specific and unique individual has communicated with another individual or group of individuals.

Telephone Toll Records

The table below represents actual telephone toll records of a member of EFF's staff, obtained with his consent from Bell Atlantic[15].

```
202 222 2222      JUL 17 94 *IC      LIVE  P     7     B     26 1FR
JONAH SEIGER                         PB 8146 RT 45     AC 2-00      DEP 5
APT XXX                       R1      INCL 300  CT     DDI 123456   LUC
XXXX XXXXXXX RD NW            R2 8147 NT C      NOB    TAX F-L-S    LCR 12
WASHINGTON DC 20009-2015      CI ELECTRONIC FRONTIER FOUNDATION STAFF 347-
                           5400

   ----AT&T----
NO      Amount  Place          Number         Date     Time     RATE  Min
1         4.62  SAN FRAN   CA  415 555-5555   JUN 18   1225P    *N     30   J8J1
2          .14  DETROIT    MI  313 555-4545   JUN 18    434P    *N      1   J8J1
3         4.00  OSSINING   NY  914 555-2323   JUN 20    826P    *E     25   J8J1
4         5.25  DETROIT    MI  313 555-4545   JUN 22    900P    *E     30   J8J1

RP    NOTATION                 TYPE PN  ACT  FU  BD  CMT-TIME  0974
```

These records indicate the date, number dialed, its location, time, and duration of calls made from 202 222-2222, which is billed to Jonah Seiger. These records do **not** indicate that Jonah Seiger himself actually placed the calls, the identity of the recipients, or the nature of the communication (i.e, voice, modem, fax, etc).

---

[14] All commercial on line services (AOL, Compuserve, Prodigy, etc), as well as most Internet providers require users to enter a password each time they log onto the service. Passwords are unique to each individual (similar to a PIN number used for cash machines at Banks), and in most cases the practice of using another persons password without permission is considered a breach of contract or user agreement.

[15] The dialed numbers have been changed . The information described above has been certified by Bell Atlantic to be identical to information obtainable by law enforcement officers with proper subpoena authorization. Records indicate long distance toll calls. According to Bell Atlantic, only long distance dialed number records are collected. Law enforcement must use pen register or trap and trace devices to capture local dialed number records.

Electronic Mail Logs

The table below represents actual electronic mail logs from the Electronic Frontier Foundation's electronic mail server. These logs indicate a message sent by an individual user (in this case, djw@eff.org) to members of an online discussion titled <eff-crypto> (EFF's online forum on issues relating to cryptography and digital privacy in general). Although this example contains addresses unique to EFF, virtually all electronic mail software logs transactions in an identical way. In the course of accounting and processing electronic mail messages, the mail server assigns each message a unique message ID number. By tracking a message ID number, one can easily know who sent a message, and to whom that message was sent. (For ease of reading, line numbers have been added, and message ID numbers are indicated here in **bold face type**).

```
01 7/29 08:15:48 IIA12559: from=<djw@eff.org>, msgid=<199407291215.IIA12559@eff.org>
02 7/29 08:15:49 IAA12559: to="|/usr/local/etc/cryptoarchiver" stat=Sent
03 7/29 08:15:50 IIA12559: to="|/usr/local/etc/dmail2list eff-crypto eff-crypto-exploder"
04 7/29 08:15:51 IIA12565: from=owner-eff-crypto, msgid=<199407291215.IIA12559@eff.org>
05 7/29 08:15:51 IIA12565: to=gnu@toad.com (John Gilmore), delay=00:00:01, stat=queued
06 7/29 08:15:51 IIA12565: to=mkapor@kei.com (Mitchell Kapor), delay=00:00:01, stat=queued
07 7/29 08:15:51 IIA12565: to=jberman@eff.org (Jerry Berman), delay=00:00:01, stat=queued
08 7/29 08:15:52 IIA12565: to=jseiger@eff.org (Jonah Seiger), delay=00:00:01, stat=queued
09 7/29 08:15:51 IIA12565: to=djw@eff.org (Danny Weitzner), delay=00:00:01, stat=queued
```

The table above follows a message sent by <djw@eff.org> to the recipients of the <eff-crypto> mailing list. Line 01 indicates that message IIA12559 was sent by <djw@eff.org>. Line 03 indicates that that message was sent to the address <eff-crypto>. line 04 indicates that message IIA12559 was sent from <eff-crypto> as message IIA12565. Lines 05 through 09 indicate that message IIA12565 was sent to specific individual recipients of the <eff-crypto> list.

Comparison of Telephone Toll Records and Electronic Mail Logs

From these two examples, it is clear that electronic mail logs reveal a great deal more about both the destination and substance of a communication than does a telephone toll record. While the telephone toll record does show that a specific number was dialed at a certain time, it reveals nothing else about the nature of the communication, or the identity of the sender or the recipient. There is nothing inherent in a toll record to indicate that a specific individual communicated with another. In the example above, we only know that 202 222 2222 dialed 313 555-4545 on a certain date and time.

In contrast, because each electronic mail address is linked directly to an individual with a password unique to that address, a record of a communication in this medium indicates the occurrence of a communication between two specific individuals. Moreover, in the example above, the log reveals that an individual communicated with a group of individuals who belong to a subject specific group (in this case <eff-crypto>). Through a simple analysis of message identification numbers, one can very easily track the communications of one person, and know with certainty with whom that person is communicating.

Appendix B

File Transfer and Retrieval Logs

Tracing a File Directly to an Individual

Virtually all online information services, such as America On Line (AOL), Prodigy, Compuserve, and the Internet, contain a wealth of files and information in areas known as "file archives". There are many thousands of archives throughout cyberspace, containing files ranging from political information (e.g.: White House press releases, legislation, policy statements, etc.), shareware (free, public domain software), to images from the Hubble Space Telescope. Users can access file archives through a variety of ways depending on the service they subscribe to.

For purposes of maintenance, accounting and security, most online services keep records of all transactions involving file transfer and retrieval. Through a simple analysis of these records, one can easily trace a file directly to an individual user.

The example to follow will illustrate how such a trace can be accomplished using transactional records from the Internet File Transfer Protocol (ftp), the primary method for transferring and retrieving files over the Internet. FTP provides any Internet user with the ability to retrieve files from any computer on the network. Files available via ftp are stored in **'ftp archives'** which can be accessed by a user through the execution of a few relatively simple commands.

Every user on an online network is identified by an electronic identity, usually identical to their electronic mail (email) addresses. Individuals control access to their email addresses through a secret personal password. Because email addresses are tied to individual users, and because ftp logs indicate that a specific file has been retrieved, a simple analysis of ftp logs can easily reveal that an individual has retrieved a specific file.

FTP Transaction logs

This example will trace an individual user's retrieval of a file from the online archives of the Electronic Frontier Foundation (EFF). The file, named **'digitel.faq'**, contains answers to frequently asked questions about the Digital Telephony legislation. The records below are actual records from EFF's ftp archive (named <ftp.eff.org>) and main computer (<eff.org>)

All computers connected to the Internet have names. In this example, it is important to note that <ftp.eff.org> and <eff.org> are two distinct computers. The computer <ftp.eff.org> keeps separate records from the computer <eff.org>. Furthermore, each authorized user has a unique electronic identity, usually same as that individual's electronic mail address (e.g.: brown@eff.org is the user Dan Brown [EFF's system administrator]). A simple correlation of the timestamps on the transactions between the two computers will reveal that Dan Brown retrieved the file **'digitel.faq'**.

I. Dan Brown Logs Onto <eff.org>

By examining the logs of the computer eff.org, we can determine when a specific individual logged onto and off of the network. This record is displayed below:

```
#  User  Terminal   Remote machine  Timestamps

05 brown    ttyp0    elec.eff.org    Fri  Jul  29  12:59:04  -  13:03:14
```

Because the user 'brown' is linked to Dan Brown through a unique personal password, this record indicates that Dan Brown was logged onto <eff.org> on Friday July 29 between 12:59 and 13:03.

II. Dan Brown Executes a File Transfer (ftp)

By examining the logs which record the programs run by users on <eff.org>, and noting the times at which those programs were run, we can determine when Dan Brown executed a file retrieval program (ftp). This record is displayed below (`printed on July 29 at 13:15`):

```
#  program   user name    terminal    start time      end time

08 ftp        brown       ttyp0        13:00:21        13:01:20
```

Note that the start and end times correspond to the period of time Dan was logged onto <eff.org>. This record clearly shows that Dan Brown ran the file retrieval program (ftp) between 13:00:21 and 13:01:20.

III. Logs from the File Archive Show a File Transfer

We now turn our analysis to the records of the computer containing EFF's online file archives (the computer named <ftp.eff.org>). Again, a simple check of timestamps reveals that a user from <eff.org> made a connection using the file transfer program (ftp). These records are displayed below:

```
#  Timestamp           Hostname     Process ID     Message

04 Jul  29  13:00:21 ftp.eff.org in.ftpd[5458]:  connect  from  brown@eff.org

12 Jul  29  13:01:20 ftp.eff.org ftpd[5458]:      FTP  session  closed
```

Note the direct correlation between the times indicated above and the times indicated on the previous two logs. This log shows that the file transfer program run by Dan Brown was executed on the computer <ftp.eff.org>, indicating that Dan Brown retrieved a file from EFF's online file archive.

IV. Logs from the File Archive Name the File Transferred to Dan Brown

One final check of the logs from EFF's online archive show which file Dan transferred to his own computer. We already know that Dan was logged onto the network between 12:59:03 and 13:03:14. We also know that he ran the file transfer program between 13:00:21 and 13:01:20. This has been confirmed by logs from two separate computers. By examining one additional log on the computer containing EFF's online file archive (<ftp.eff.org>), we can see which particular file Dan retrieved. This log is displayed below:

```
Fri  Jul  29  13:01:18  1994 1
                  eff.org
                              67773
   /pub/EFF/Policy/Digital_Telephony/digitel.faq .
```

This log shows that the file **'digitel.faq'** was retrieved at 13:01:18 by a user logged onto the computer <eff.org>. Note that the exact time of the file retrieval corresponds to the time that Dan Brown was running the file retrieval program (as indicated on the logs described previously).

We have seen that Dan Brown was running the file retrieval program between 13:00:21 and 13:01:20. This is confirmed on the logs from both the computer Dan was logged onto (<eff.org>) as well as the computer containing the online file archive (<ftp.eff.org>). Because the logs also show that the only user running the file transfer program at that time was Dan Brown, we have now confirmed that Dan Brown retrieved the file **'digitel.faq'**.

FTP Logs Reveal the Actions of an Individual User and the Contents of those Transactions

Detailed transactional information from online information services enables anyone with access to these records to reconstruct a detailed picture of a user's actions. In this case, the logs show which document the user accessed. Because all users on the Internet and other online services are linked to their electronic identities by a unique password, transactional records which reveal the electronic identity of a user correspond directly with that individual. The electronic identity <brown@eff.org> is always Dan Brown. In the case of this example, transactional records reveal that Dan retrieved the file **'digitel.faq'** from the online archives of the Electronic Frontier Foundation.

Transactions similar to the one illustrated here occur millions of times each day on computer networks throughout the United States. Furthermore, because computer logs record each and every transaction, it is not difficult to track the actions of any individual using an online service simply by examining such logs.

This type of detailed transactional information is not unique to Internet ftp sessions. It is captured in similar forms on computers throughout the online service world. Every time a user logs on to an online service, sends electronic mail, retrieves a file, or joins a discussion group, detailed information is collected in the normal course of completing these transactions. And, since virtually all users of online services are personally linked to their electronic identities by a unique password, all of these transactional records point directly to the actions of individual people.

PODESTA ASSOCIATES, INC.,
Washington, DC, May 29, 1991.

Hon. DON EDWARDS,
Subcommittee on Civil and Constitutional Rights,
House Office Building, Washington, DC.

DEAR CONGRESSMAN EDWARDS: Enclosed please find a copy of the Final Report of the Privacy and Technology Task Force. The task force was appointed by Senator Patrick Leahy, Chairman of the Senate Subcommittee on Technology and the Law, and consisted of 15 members representing a wide array of business, consumer and privacy interests and experience. The task force was charged with examining new technologies and determining the adequacy and effectiveness of the protections found in current federal law (most notably in the Electronic Communications/Privacy Act).

While task force members disagreed—at times, strongly—on many issues, we reached consensus on many others. I believe the report raises a number of issues which may be of interest to you, and makes recommendations where possible, presenting alternate viewpoints where consensus was not reached. We delved into many complex and controversial issues facing society today: the privacy of new radio-based communications technologies, Caller ID, government wiretapping, dossier building, restrictions on the dissemination of customer proprietary network information and appropriate uses of information derived from phone calls to 800 and 900 numbers.

I hope you find the report useful.

Sincerely,

JOHN D. PODESTA,
CHAIR,
Privacy and Technology Task Force.

FINAL REPORT OF THE PRIVACY AND TECHNOLOGY TASK FORCE SUBMITTED TO SENATOR PATRICK J. LEAHY

INTRODUCTION

In August 1990, Senator Patrick Leahy chaired a hearing of the Senate Judiciary Subcommittee on Technology and the Law. The hearing focused on Caller I.D. technology and the Electronic Communications Privacy Act (ECPA). At that hearing, Chairman Leahy became convinced that developments in the area of communications technology required a review of ECPA to ensure that the privacy protections within the statute had not been outdated by new technology. Senator Leahy was interested in an array of perspectives, so a task force was assembled with experts from a wide variety of fields: technology, business, consumer advocacy, the law, and civil liberties. (A list of members is provided in the appendix.) While the group was diverse, it was not constructed for, nor did it hold itself out as, representing every interest or view.

The task force was charged by Senator Leahy with examining current developments in communications technology and how they relate to the legal framework for protecting communications privacy. This examination was to focus on the extent to which the law in general, and ECPA, specifically, protects, or fails adequately to protect, personal and corporate communications privacy.

The task force studied a variety of newer communication media: cellular phones, personal communications networks, the newer generation of cordless phones, wireless modems, wireless local area networks (LAN's), and electronic mail and messaging. The task force also debated newer technological innovations with a focus on digital transmission of information and out of band communication signalling which is capable of carrying Calling Party Number with a privacy indicator. The task force also considered whether special privacy concerns were raised by the increased service offerings of Caller I.D. and 800 and 900 numbers. The task force examined the extent to which these technologies were regulated by the federal government, either through ECPA or the Communications Act of 1934 and whether they were regulated by state authorities. The task force discussions usually centered on the appropriate balance between privacy rights of one or both of the parties to the communication and the rights of the called party or a third party to employ devices which capture either the substance of a communication or detailed transactional information about the fact of the communication or the parties to it. The task force also discussed the extent to which the government had a right to monitor communications or obtain information about the communicants, by request, by subpoena, or by warrant.

As a starting point, the task force agreed that traditional privacy principles, embodied in the Constitution, must guide public policy with respect to communications privacy and the new technologies. Few social and commercial relationships remain unaffected by the introduction of new technologies such as cellular and cordless phones, electronic mail, bulletin boards, and pagers. Traditional barriers of distance, time, and location are disappearing as our society comes to take these advanced forms of communication for granted. As new technologies become available, a tension is often created between existing societal values and expectations, and the commercial opportunities and outlets for personal expression created by these advances.

The task force agreed that peoples' expectations of privacy should not be measured against what is technically possible. People care deeply about their privacy, and cherish the ability to control personal information. Even if they have done nothing wrong, or have nothing to hide, most people are offended if they are denied the ability to keep certain personal information confidential. Crucial to one's sense of self is the right to maintain some decision-making power over what information to divulge, to whom, and for what purpose. The uses of new technologies are always threatening to overtake current law, leaving society without a new set of laws and social mores to limit and define the extent to which new devices can be used to know all we can about each other, often without regard to each other's wish to keep information private.

National polls document a growing public demand for privacy protection. A *Trends and Forecasts* survey released in May 1989 found that seven out of ten consumers feel that personal privacy is very important to them, with many expressing the fear that their privacy is in jeopardy. Half of the people believe new laws are needed to protect their privacy. A May 1990 Harris study concluded: "Particularly striking is the pervasiveness of support for tough new ground rules governing computers and other information technology. Americans are not willing to endure abuse or misuse of information, and they overwhelmingly support action to do something about it."

After examining a wide array of technologies, and considering the privacy implications of them all, there were significant points of agreement among task force members. However, the task force did not reach consensus on every question. The goal of this report is to set out points of agreement, to describe areas of controversy, and to recommend areas in need of further examination by the Subcommittee.

Emerging communications technologies and the extent of protection by the electronic communications privacy act of 1986

In 1984, Congress undertook to update the 1968 Wiretap Act to extend coverage to new forms of telecommunications. The effort culminated in the passage in 1986 of the Electronic Communications Privacy Act (ECPA). The 1968 Wiretap Act generally limited its protections to voice communications carried on a common carrier network. The 1986 Act expanded protection to voice and nonvoice electronic communications, whether carried on common carrier or through a private network. Title I of ECPA 1) protects wire (voice) or electronic communications, while in transmission, from illegal interception by unauthorized third parties, 2) creates standards and procedures for court authorized electronic surveillance, and 3) regulates when electronic communications firms may release the contents of communications during the transmission process. Title II of ECPA provides legal protection of the privacy of stored electronic communications, from both outside intruders and unauthorized government officials. By helping to ensure the confidentiality of electronic communications, ECPA encourages the development and use of new technologies.

ECPA has served as the foundation for legal protection of the privacy of electronic communications. However, five years after ECPA was enacted, a new array of technologies, which were only on the drawing board in 1986, are in the process of being deployed. These new technologies have highlighted the need for a review of the 1986 Act. Specifically, the task force perceived four trends which are challenging the existing statutory scheme for communications privacy: 1) There are a number of new radio-based communications technologies that are in the process of being deployed, that facilitate voice, data, and broadband communications, but that do not fall clearly within the protections afforded by ECPA; 2) There is a movement away from analog to digital transmission, digital being more easily protected at a lower cost; 3) Signalling System 7 which is in the process of being deployed by many of the nation's telephone companies, employs out-of-band signaling, and thereby creates both an opportunity for new services and enhanced concerns about the privacy of transactional information; and, finally, 4) customer premises equipment (CPE) can now perform a wider variety of functions which can be used to enhance or defeat privacy protections.

In analyzing these trends, the task force focused on the proper balance between the promise of these new technologies and the privacy rights of those who use electronic communications equipment. The report will summarize the task force's conclusions, concerns and points of controversy in five major areas:

I) New Radio-Based Communications Technology and whether the content of communications carried on these technologies is or should be protected by federal law.

II) Out-of-Band Signaling and new service offerings and the related privacy risks from disclosure of transactional information (especially the calling party's number).

III) 800 and 900 Numbers and the appropriate use of customer information obtained by businesses employing these technologies.

IV) Electronic Mail and concerns about the privacy of electronic messages carried on private networks.

V) Government Monitoring and the special concerns raised by the government's action, where it has obtained a valid warrant, to segregate and monitor specific communications.

I. NEW RADIO-BASED COMMUNICATIONS TECHNOLOGY

The Electronic Communications Privacy Act updated the 1968 Wiretap Act to deal with two major trends that were sweeping the telecommunications industry. First, ECPA broadened coverage from voice only to other forms of communication, including data and video. Second, ECPA expanded coverage from communications common carriers to all electronic communications whether or not carried by a regulated common carrier.

The new law failed to anticipate fully the expansion of the number and kinds of private communications that can and will be carried by "wireless" systems where some or all of the communication is carried by radio link. While the drafters of ECPA considered and drew distinctions between "cordless" and "cellular" phone technologies, the full range of potential service offerings was not well understood at the time.

The anticipated increase in the provision of such radio-based services and networks could dramatically change the current make-up of this country's telecommunications infrastructure and provide telecommunications consumers with added efficiency, cost-savings, and mobility. Radio-based communications may well displace many communications now carried on "wire" systems currently protected by federal law. Such communications will not fall neatly into the distinctions drawn by ECPA.

ECPA makes a key distinction between communications that are "readily accessible to the general public" and those that are not.

Communications that are not readily accessible to the general public are protected, i.e., it is illegal to intentionally intercept such communications and any electronic surveillance carried out by government officials must be in compliance with ECPA, which generally requires court authorization, high-level administrative review and procedural safeguards.

Communications that are "readily accessible to the general public" are not protected, i.e., it is not illegal to intercept the communication and government officials can monitor and use as evidence the content of the communication without first obtaining a warrant.

With regard to radio-based technologies, ECPA sets out a definition in the negative, i.e., it defines specific communications that are not readily accessible to the general public. Section 2510 (16) states: "readily accessible to the general public" means, with respect to a radio communication, that such communication is not—A) scrambled or encrypted; B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication; C) carried on a subcarrier or other signal subsidiary to a radio transmission; D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio * * *.

In addition to drawing the above distinctions between communications which are not readily accessible to the general public, ECPA exempts from its coverage "the radio portion of a cordless telephone that is transmitted between the cordless telephone handset and the base unit." 18 U.S.C. Section 2510(1) and (12)

The drafters of ECPA relied on distinctions between communications technologies which, in 1986, made it difficult to intentionally target and monitor specific communications (where a reasonable expectation of privacy could be said to exist) and those in which the communication was "out in the clear", where specific monitoring was easily achieved and where no *reasonable* expectation could be found.

The drafters of ECPA recognized that there were no bright line tests in this area. For example, the Committee reports of both the House and Senate recognized that radio equipment was available to the public that was capable of receiving cellular telephone conversations at the time the Act was passed. Because of the complexity of the cellular telephone system, however, including the number of channels and the ability to frequently change frequencies, the ability to monitor specific conversations was thought to be difficult—a judgment confirmed by law enforcement officials at the time. In contrast, cordless phones, because of the fixed location of the base unit and constant frequency, could be easily targeted and monitored. Thus, no protection was afforded to that technology.

The task force examined a host of new communications offerings which have been proposed to carry personal communications to determine whether they were in fact covered by the current definitions of the statute and if they were not, whether they should be protected both legally and technically against government and intentional private surveillance. A list of those technologies and the task force's analysis follows.

Cordless Telephone 2 (CT2; Telepoint): This technology utilizes a series of public base stations which can be accessed by a personal handset if the phone is within a short distance from the base station. Such systems are currently being deployed in the U.K., where they serve as an alternative to coin pay phones. Some experimental licenses have been issued in the U.S. They also can be used in public buildings such as hospitals, convention centers, etc., where users have the flexibility to roam within a prescribed area, but retain access to the phone system. Calls must be outgoing; incoming calls can not be received by the handset. The technology currently uses analog transmission but is moving towards digital transmission. Random monitoring of conversations would be possible with a receiver placed within 150 to 200 feet of the base stations. Targeted monitoring of specific conversations would be difficult. The task force was of the view that the technology could be found to fall within the ECPA's exception for cordless phones. The task force was of the view that such communications should be legally protected from unauthorized Interceptions by ECPA, and that the government should obtain a warrant before monitoring conversations.

Personal Communications Network (PCN/PCS): Still in an embryonic stage of development, the concept of PCN/PCS envisions the use of portable, pocket-sized handsets capable of initiating and receiving communications regardless of the user's location at any point in time. As a result of improvements in both telecommunications and computer technology, the handset will be able to signal its location to the network so that incoming calls can be routed on a national, perhaps international, basis. The majority of experimental licenses issued by the Federal Communications Commission (FCC) anticipate the use of digital technology. Thus, interception of specific conversations will be difficult. The task force was of the view that this type of communication should be protected by ECPA, since the current generation of cellular technologies is protected. Some question remains, however, as to whether the law could be interpreted to permit PCN to fall within the exception from coverage for cordless phones. A clarification of the law to make certain that such communications are legally protected against unauthorized interception is recommended.

Specialized Mobile Radio (SMR) system operations: The FCC recently took action to allow an existing SMR operator (Fleet Call, Inc.) to proceed with its plans to construct and operate on a private carrier basis "enhanced" SMR systems in the top six markets in the U.S. As proposed, the new system configurations incorporate the basic design concepts embodied in the provision of public cellular mobile service, i.e. frequency re-use/call hand-off between transmitting cell sites. In addition, the systems will employ digital technology. As such, unauthorized monitoring of specific communications will be difficult. These systems will clearly fail outside the protections currently afforded to the public cellular systems under ECPA because they will operate on private land mobile frequencies. *See* Section 2510 (16)(D). The task force concluded that no meaningful technological distinctions, which would warrant a different treatment of privacy rights under ECPA, exist between public carrier cellular systems and this new limited class of SMR cellular systems. if such systems are to be deployed, ECPA should treat cellular systems, whether provided by a common carrier or private system, as "not readily accessible to the general public."

Cordless Telephone 3 (CT3, radio PBX): Technology exists to construct office buildings with a mini-cellular switching system inside the building. Such a system can be utilized to avoid the costs of rewiring a building when the office structure is reconfigured. Such a system can provide businesses with flexibility and cost savings when deploying telecommunications instruments. Under the current ECPA structure, however, such radio-based PBX systems would probably fall within the exception for cordless telephones, and therefore, a business or individual utilizing this technology could be legally unprotected from unauthorized interception of their communications. The task force Is of the view that such legal protection should be afforded.

Wireless Data Communications: Computer companies are experimenting with, and seeking FCC licenses for, "wireless" modems which can transmit data between computers without the computers being wired together, either directly or through phone lines. Such modems will have applications in several environments including the transmission of data from remote sites (a kind of cellular laptop computer) as well as within an office environment (wireless local area network or LAN). Under ECPA, the answer to the question whether such communications will be legally protected from unauthorized interception will depend on where, within its regulatory structure, the FCC decides to allocate spectrum for these uses and whether the communication is encrypted or the digital means used for such communications qualifies for protection under Section 2510(16)(B) relating to modulation techniques that are not readily accessible to the general public. Under current FCC proceedings, there is a likelihood that such communications will not be protected unless the user goes to the expense of full data encryption. The task force recommends appropriate amendments to legally protect digital communications of this type from unauthorized Interception.

Cordless Telephones: The discussion of these newer technologies led the task force to a lengthy discussion of the premise of the 1986 Act that "the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit * * *" should be exempt from coverage of the Act.

The task force first considered some newer technological developments which make communication carried on cordless telephones somewhat more secure. Cordless phones have reduced the transmission power so that the phenomenon of having calls blast through on an FM radio receiver has been eliminated. Cordless phones also have begun to utilize technology which permits the call to be carried between the handset and base unit on more than one frequency. This feature can and is available to add security and privacy to the phone call. The next generation of phones will utilize digital transmission technology which will make unauthorized interception more difficult.

Perhaps the most important change since 1986, though, is not technological but societal. The cordless phone, far from being a novelty item used only at "poolside," has become ubiquitous. A leading telephone equipment supplier now sells as many cordless telephone units as wired sets. It is projected that cordless phones will be in use in 68 percent of American households by the end of the decade. More and more communications are being carried out by people in private, in their homes and offices, with an expectation that such calls are just like any other phone call. Given such technological changes and under such societal circumstances, the task force concluded that to relieve the government of the duty to obtain a warrant before monitoring such communications is to vitiate much of the protection which should be afforded to communications privacy by the federal wiretap law and the Fourth Amendment. Therefore, the task force recommends that consideration be given to elimination of the exemption for cordless phones, while preserving an exception for unintentional or accidental private party interception.

In recommending both the maintenance and extension of legal protection for "wireless" radio communications, the task force is aware that inexpensive, widely available scanners and other devices are available that make it possible to intercept radio communications. The task force strongly believes that such technologies should not defeat citizens' reasonable expectation of privacy against government intrusion and that government agents should conduct electronic surveillance of the technologies described above only under appropriate court authorization. At the same time, criminal sanctions could be overbroad in criminalizing inadvertent and unintentional interceptions of radio communications by persons with access who legally possess and use scanner and other devices that intercept radio communications. The existence of monitoring devices makes it difficult to rely solely on legal protection against third-party eavesdropping. The task force is aware that legal protections may not go far enough in affording citizens real privacy protection against intentional but undetected private surveillance. For example, concerns were expressed by a number of task force members that technical privacy enhancing features for radio-based systems should be more rapidly deployed by manufacturers and service providers.

To rectify this situation, the task force does not want to overcriminalize in this area, i.e., penalize unintentional conduct. The task force Is of the view that the rights of private citizens using radio scanners can appropriately be addressed by clearly setting forth specific intent requirements in the Act, by tying the criminal penalty to targeted surveillance of specific communications and by further adjusting the civil and criminal penalty structure of the Act, rather than exempting whole categories of telephone technologies and thus making them fair game for monitoring by government agents without a warrant, corporate spies, or just plain snoops.

Second, in order to ensure that citizens both understand the vulnerability of particular radio technologies to private, intentional, illegal interception and to encourage industry to develop and market communications devices that are less vulnerable to intrusion, the task force endorses the concept that ECPA should be amended in such a way as to encourage the placement of warnings and notice of the vulnerability of customer premises telephone equipment on specific CPE and that manufacturers be encouraged to make consumers aware of the technical levels of privacy on different types of equipment. The task force believes this will encourage industry to compete with each other in developing devices which are more secure. The task force believes Congress should work with the FCC, Industry, and technical experts to further explore ways to enhance the security of different types of equipment and to further explore ways to enhance consumer awareness of the security of different types of equipment and laws pertaining to communications privacy. In particular, the task force recommends the examination of encryption technology and its potential impact on enhancing the privacy, security, and authenticity of electronic communications. The task force further encourages communications service providers to continue to explore the incorporation of encryption and other privacy enhancing features in new communications services, so as to improve communications privacy.

II. OUT-OF-BAND SIGNALLING

Telephone transactional information caller I.D.

Prior to 1976, telephone calls were processed between telephone company offices using signaling information on the same trunk as the voice or talk path between the offices. This type of signaling is referred to as "in-band" because it is an inherent part of the path on which the call is carried. Part of the information contained in this signaling is Automatic Number Identification (ANI), which allows the automatic identification of a calling station for billing purposes. The use of ANI allows telephone subscribers to dial directly a toll call without operator involvement.

However, transmitting signaling information over voice circuits is inefficient. In order to improve network efficiency, a new interoffice signaling technology called Common Channel Interoffice Signaling (CCIS) was introduced. CCIS was the precursor of today's Common Channel Signaling 7 (CCS7). Instead of processing interoffice calls using a common path for both signaling and voice, the CCS7 network allows signaling information to be sent through a separate high speed data network before calls are connected between offices. This type of signaling is known as "out-of-band" because it does not utilize the same facilities for the transmission of call processing information as are used for connecting the call. CCS7 signaling information contains routing information (where does the call go?), translations (does the dialed number equate to something else?, as is the case with an 800 number), billing, and calling party information (where did the call come from?). The calling party information is similar to ANI in that the calling party's number is automatically identified. However, unlike ANI, because the information is part of a data stream, CCS7 also has the capability to provide a "privacy indicator" to flow along with the other call processing information in the data stream. The privacy indicator makes it technically possible for calling parties to block the release or display of information outside the network. However, the information blocked can still be used within the network for billing and routing purposes.

CCS7 has the capability to provide blocking in two ways: per-call or per-line (also known as subscription blocking). Per-call blocking allows the calling party to dial a code, before a call is placed, to indicate that, for a particular call, the Calling Party Number (CPN) should not be disclosed to the called party. If per-line blocking is available, the calling party need not dial a code prior to the call; CPN is automatically withheld from the called party. Both options prevent CPN from being disclosed to the called party, but neither prevents delivery of billing information to the interexchange carriers (whether via ANI or CPN).

As CCS7 began to be deployed, phone companies began to offer a service known as Caller I.D., Caller I.D. allows telephone subscribers to see the telephone number of the person calling before they answer the phone. In order to have the number displayed, telephone company offices must be equipped with CCS7, customers must subscribe to the service, and customers must buy either a number display unit to connect to their existing telephone or a special Caller I.D. telephone. When a call is delivered to the called party, the telephone number of the calling party is displayed on the screen.

ECPA prohibits "trapping and tracing" of information regarding the origination of electronic communications. A trap and trace device is defined (18 U.S.C. Section 3126(4)) as "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." This prohibition has three exceptions.

Trapping and tracing is permitted in order to operate, maintain, and test the communications service; to record the beginning and end of communications for billing or other similar functions; and, in those instances "where the consent of the user of that service has been obtained." (18 U.S.C. 3121(b)).

There is a sharp division of views among task force members on whether Caller I.D. is a trap and trace device as defined in ECPA. The only court to rule on this question is the Commonwealth Court of Pennsylvania which held that Caller I.D. constituted a trap and trace device under state law which paralleled ECPA. There is a further division of views on the question of whether the customer or the service provider may employ a trap or trace device where the consent of the user has been obtained.

As phone companies began to market Caller I.D., privacy and consumer advocates argued that the right to control the disclosure of a subscriber's phone number should not be transferred to the telephone company. They said that the service violated ECPA, and they advised policy makers to require that phone companies provide free "blocking," on either a per-line or per-call basis.

Initially the Caller I.D. debate took place before state public utility commissions, as phone companies sought authorization to provide Caller I.D. through tariff actions. The policy decisions have varied widely from state to state. New Jersey permits phone companies to offer Caller I.D. without any call-blocking service. Neighboring New York is considering a PUG regulation which would require that all customers with unpublished numbers automatically be given a blocked line. D.C. permits Caller I.D. but requires that per-call blocking be made available to the calling party at no charge. California has enacted legislation authorizing Caller I.D. but requiring that per-call blocking be offered to calling parties.

In Pennsylvania, the Commonwealth Court found that Caller I.D. violated both the state wiretap statute, a law virtually identical to ECPA, and the state constitutional right to privacy. The Court also found that the proposal to provide a blocking service to particular phone subscribers lacked minimal due process standards and was therefore unconstitutional. (*Barash* v. *Pennsylvania Public Utility Commission,* Commonwealth Court of Pennsylvania No. 2270, May 30, 1990). That case is on appeal to the Pennsylvania Supreme Court.

The task force recognized that there were privacy interests of both calling and called parties that any public policy on Caller I.D. must recognize. The task force noted, however, that in calls to 800 and 900 subscribers, the called parties had no such privacy interest.

Consumer and privacy advocates said that Caller I.D. would undermine privacy as the right to control the disclosure of personal information was transferred from the phone subscriber to the phone company. They said that the benefits of Caller I.D. for residential phone subscribers had been greatly overstated, that answering machines were a less expensive, less intrusive, but far more effective way to screen incoming calls. They also said that the Call Trace service provides all the safety benefits of Caller I.D. without placing the subscriber in the dangerous position of responding directly to harassing phone callers. They said that "balancing" the privacy rights of call originators and call recipients was a false characterization of the service since the privacy rights of both parties could be easily accommodated.

Opponents of blocking, such as Bell Atlantic, believe that if Caller I.D. is available without blocking, it will achieve the greatest deterrent impact on anonymous, obscene, harassing, and threatening calls. Bell Atlantic has presented congressional testimony supporting the deterrent value in the availability of Caller I.D., a benefit which accrues even to those who do not subscribe to Caller I.D.. Bell Atlantic states that Caller I.D. broadly serves the public's right to be let alone and gives recipients of telephone calls the same information that callers have—the number of the person to whom they are speaking. They further argue that there are ways other than blocking to address the unique needs of groups with a need to prevent identification, i.e., domestic violence and law enforcement agencies, etc., and telephone companies have worked with these groups and have successfully provided alternatives, other than blocking.

The task force was split among four different viewpoints. The first group was comprised of some of the consumer and privacy rights advocates. This group was of the opinion that, taken as a whole, the Caller I.D. service would greatly reduce the privacy rights of all phone subscribers and should not be encouraged. This group believes that phone subscribers should not take any additional steps to protect their current expectation of privacy, and that therefore free, per-line blocking should be available and that should be the rule unless the calling party chooses to disclose his number.

The second group was comprised of other consumer and privacy advocates, as well as those members who generally represent businesses that are not telephone companies but which use the telecommunications network for marketing and other purposes. This group is of the opinion that provision of per-call blocking should be mandatory and that there should be federal legislation establishing this protection as a floor. Some advocates of per call blocking believe that federal preemption may be desirable in order to have a national standard that would minimize customer confusion. They believe that per line blocking may well inhibit the development and deployment of new services and encourage caller rejection schemes, reducing the utility of the telecommunications network.

The third group, comprised of a number of phone company representatives, holds the view that per-call blocking is the appropriate policy option, but that no federal legislation is necessary, that this issue is being adequately handled by the states.

The fourth group, comprised of the remaining phone company representatives, favor unrestricted Caller I.D. because they believe that it restores full accountability when using the public telephone network. Some are of the view that federal legislation is not appropriate because each state should be free to adopt the regulatory policies which it believes are best suited to the needs of its residents, and that in fact Caller I.D. has been offered successfully in five states without blocking. Studies based on those experiences show that it reduces unwanted calls for all customers, not just those who subscribe to the service. Others have the view that if Congress decides to adopt blocking legislation, then per-call is preferable, with federal preemption of stricter state regulation.

Conclusion: The task force studied the new signaling technologies, discussed the issue in depth, examined the law, yet was unable to reach any consensus on what, If any, legislative change is necessary.

III. 800 AND 900 SERVICES

The task force was particularly concerned about the use of services that disclose Calling Party Number in the commercial setting, such as the use of ANI for 800 and 900 services. The task force noted that while an 800 or 900 service has a business interest in the calling party number (from both a financial and productivity perspective), it also has an obligation to respect the privacy of the calling party. The task force further recognized that few consumers were aware that a call to an 800 or 900 service would result in the electronic disclosure of the caller's identity.

Some consumer advocate members of the task force were of the view that there was no necessary business reason for the compelled disclosure of the caller's identity since this information could be obtained, with the knowledge of the caller, by simply asking for it.

Various members of the task force observed that services provided through 800 and 900 numbers may differ in significant respects (such as who pays for the call) and, accordingly, that some distinctions might appropriately be made with respect to the relative need of providers of such services for information regarding the identity of the calling party.

The task force spent considerable time discussing privacy concerns raised by the disclosure of the calling party's number to businesses and services utilizing 800 and 900 telephone number technology. Many 800 and all 900 line service users lease lines from inter-exchange carriers. When a call is completed by some interexchange carriers to an 800 or 900 service, the call may be handed off to the service with information necessary for call completion, i.e. either CPN or ANI. The calling party's number is thus mechanically disclosed to the 800 or 900 number service, where it can be used for billing and routing, account management and security purposes. The task force's discussion focused on the appropriateness of 800 and 900 services using that information disclosed for one purpose (call completion and billing) for other purposes (generally marketing) without the consent of the calling party. In the future, CSS7 will allow the caller's identity *and* his privacy preference to be disclosed.

As signalling system 7 (SS7) is implemented through the country, by both local exchange and inter-exchange carriers, Calling Party Number and the ability to block will be available for long distance and 800 and 900 numbers. Task force members have a wide variety of opinions on whether, and under what conditions, blocking should be available (see p.12, *supra,* for an explanation of the four different viewpoints represented on the task force).

With regard to ANI, the task force recommends enactment of federal legislation or adoption of appropriate FCC rules governing the dissemination of Information by 800 and 900 services. Specifically, such a law or regulation should provide that the telephone number and information derived from ANI should not be disseminated by the 800 or 900 service provider or user without the customer's informed knowledge and ability to prevent use of their number for marketing purposes. Some members of the task force did not support this recommendation.

This approach was endorsed by the U.S. Privacy Protection Study Commission in 1977, and has been adopted in Federal legislation such as the Cable Communications Policy Act of 1984 (47 U.S.C. Section 551(c)(2)(C)) and the more recent Video Privacy Protection Act of 1988 (18 U.S.C. Section 2710(b)(2)(D)). It also is similar to the approach endorsed by the FCC for billing for nonadult services offered through 900 numbers. *Cf. In re Regulations Concerning Indecent Communications by Telephone,* 5 FCC Rcd 4926 (1990).

There were some members of the task force who asserted that no use of the ANI data should be made without the affirmative consent of the calling party. Those task force members holding this view believed that an opt-out mechanism is an inadequate privacy safeguard.

While all members of the task force agreed that some form of consent was necessary, there was disagreement over whether the consent should be opt-out or opt-in (affirmative), and what level of information was due to the customers.

While enactment of a consent requirement would be a helpful step in giving consumers greater control over the dissemination of personal information, it would not solve the problem of consumer confusion about exactly what personal information is mechanically disclosed when using the telephone or electronic communications service. That problem is, if anything, exacerbated by the availability of call blocking for some services (e.g., Caller I.D.) when it is not available for others (e.g. blocking ANI to an 800 service). Those providing electronic communications services to the public bear a responsibility to adequately inform consumers about how the system works and how they can limit the disclosure and dissemination of personal information. Some members believed that the service provider should advertise that the calling party number information will be mechanically disclosed. Such a policy has been proposed in legislative form in the State of California.

Customer prorietary network information

Section 2703(c) of ECPA affirmatively permits any provider of electronic communication service or remote computing service to disclose "a record or other information pertaining to a subscriber or customer of such service" to any person other than a governmental entity. This provision specifically does not apply to the content of such communication. A provider may disclose such information to the government only upon receipt of a subpoena, warrant or with the consent of the subscriber or customer. Thus ECPA does not restrict the dissemination of transactional data about subscribers to nongovernmental entities.

Section 2703(c) addresses only the release of subscriber information to the government when the government is not the subscriber to the service, but rather a third party. Under this circumstance, for example, a long distance carrier is restricted from providing the government with a list of persons who called an 800 number subscriber. However, when the government operates an "800" service, it may obtain the numbers of the calling parties without subpoena. Further, ECPA does not restrict the 800 number subscriber from releasing transactional information and identification of people who called the subscriber.

The Regional Bell Operating Companies (RBOC's), and AT&T are subject to additional rules on the use and marketing of customer information. These rules have been established for competitive rather than privacy protection. The most significant of these rules are the Customer Proprietary Network Information (CPNI) restrictions which arose out of the Computer II and Computer III proceedings at the FCC.

Under the FCC's rules, CPNI consists of a customer's service records and billing records. Service records include the customer's name, service location, billing address, telephone number and billing telephone number, and a description of all network services and features and the monthly charge for those services. The billing records are copies of the customer's actual telephone service bills. They include call detail for toll calls and for any local call detail services to which the customer subscribes. They also contain the number of message units a customer is charged, if message units are applicable within the customer's service area, and the number of local calls, if any, for which per-call charges are imposed.

The FCC's CPNI regulations require that the RBOC's and AT&T annually notify multi-line business customers of their right to control RBOC/AT&T access to their CPNI for purposes of marketing CPE or enhanced services.

In addition, the FCC has adopted regulations regarding an RBOC's use of "aggregated" CPNI (ACPNI). ACPNI includes any aggregated information contained in the regulated company's databases which does not identify an individual customer, which includes restricted records, and which is also not available outside of the company in commercial databases. These rules require the RBOC to make any ACPNI utilized by its enhanced service or customer premises equipment marketing personnel available to enhanced service providers (ESP's) or CPE competitors on equal terms and conditions.

CPNI regulations apply only to the seven RBOC's and AT&T (there are no ACPNI requirements for AT&T). They do not apply to any of the more than 1000 independent telephone companies, cellular carriers, interexchange carriers other than AT&T, ESP's or other business concerns involved in telecommunications and information services. The rules were drafted to lessen the competitive advantages of the RBOC's and AT&T as they implemented CPE and enhanced services on an integrated basis.

The CPNI rules are inconsistently applied in that they provide differing standards for telephone companies, for enhanced service providers, and for equipment vendors depending on whether the equipment or service is supplied by the RBOC's and AT&T or by any other entity. From a privacy perspective some members of the task force believe these are not meaningful distinctions which justify disparate treatment.

New PCN technology could elevate concerns about CPNI. Because PCN allows communication on a roving national and potentially international basis, a CPNI dossier would be all the more invasive. With PCN, an electronic communication service provider could conceivably keep a record of the exact location of both the subscriber and the calling party, in addition to the information that is now collected. With PCN, the electronic communication service provider would know a subscriber's whereabouts at virtually all times, the identity of everyone with whom he communicates by phone (either as called or calling party), his credit history, the information services he utilizes, and the 900 numbers he calls.

The task force believes that CPNI—like customer Information held by all businesses—involves sensitive personal data as well as competitively useful information.

Members of the task force representing telephone companies believe that the existing CPNI rules are consistent with the privacy expectations of their customers. Customers expect the firm with which they are already doing business to be knowledgeable about which services they have selected and to keep them Informed of new services. These members are of the opinion that It is not necessary to limit further RBOC/AT&T unregulated affiliate access to CPNI, and point out that larger ESP's have access to vast quantities of customer information from their unrelated businesses and are unrestricted in their ability to use that information. Lastly, they note that, In the event that customers do want to restrict RBOC/AT&T access to their CPNI, the RBOC's and AT&T are obligated to accept and honor such a request. This group believes that no change should be made to the CPNI rules, that the current rules meet customers' expectations of privacy by allowing them to restrict use and release of the CPNI.

Other members of the task force were of the view that from a privacy perspective all providers of communications services to the public, whether affiliated or unaffiliated with the RBOC's and AT&T, ought to be required to obtain the consent (see discussion of 800/900 numbers, p. 14, *supra*) of the telephone subscriber, including residential and single line businesses, before the CPNI about that subscriber Is used for purposes unrelated to telephone service.

IV. ELECTRONIC MAIL AND PRIVACY RIGHTS

In general, the Electronic Communications Privacy Act is serving well its purpose of providing privacy protection to electronic mail. The task force discussed various recent technical developments and policy issues, but does not suggest any change in the law relating specifically to electronic mail at this time. The issues discussed by the task force include the question of whether the law provides adequate privacy protection in the workplace, issues relating to the interconnection of various electronic mail systems, and the question whether nonpublic electronic mail service providers, such as an employer, should be obligated to give notice to affected users, such as employees, of the fact that the government has requested access to electronic mail files.

There has been some controversy, lately, regarding the nature and extent of an employer's duty to respect the privacy of electronic mail sent within the workplace by employees. ECPA does not limit employer access to electronic mail sent in the workplace, for various reasons. First, workplace systems are typically not offered "to the public" and so are not covered by ECPA's prohibitions on disclosure. In addition, electronic mail messages sent in the workplace are sent to and received by employees acting on behalf of the employer, who may therefore have a legal right to consent to access and disclosure. In addition, the employer is typically the provider of the electronic communications service and, as a result, has a general right to set the terms for use, to consent to access and disclosure, to monitor for security purposes, and so forth.

The task force recognized that access to employee electronic mail files are part of the larger issues of workplace privacy. The issues are complex but there is no strong justification to treat electronic mail fundamentally differently from many other means of communications and data storage used every day in the office. At the same time, the task force noted that in many circumstances there was a strong privacy interest in the content of an electronic message and that employees are increasingly making use of electronic mail systems that gateway to other users outside of the organization. In general, the terms on which employers can access electronic files will be the subject of policy manuals and employment agreements.

In lieu of changes in ECPA at this time, the task force recommended that employers adopt clear policies on the use of electronic mail services and provide clear notice to employees about the circumstances where access to electronic mail may be obtained. Such notice provisions are likely to avoid misunderstandings between employers and employees regarding the appropriate use of the electronic mail service. Where possible, employers are encouraged to adopt basic procedural safeguards before conducting searches of employees' mail files. Such procedures are likely to avoid litigation where an employee feels that he or she has been aggrieved by the search.

The growing use of electronic mail in the workplace, and the increasing interconnection between electronic mail systems, does pose a complex issue regarding the coverage of ECPA, however. ECPA's disclosure limitations apply to electronic communications services offered to the "public". As employers connect customers, suppliers, former employees and others, it may become more and more difficult to determine which systems are covered. In addition, messages originating on tightly controlled systems may make their way through "gateways" to electronic mail systems with far less rigorous controls on access, without adequate notice to the users of the systems. Another hybrid case posing special problems will be "private" electronic mail service accounts provided on large public systems for employees of a particular company at the employer's expense. In all these situations, it may become more and more difficult to determine whether a particular employer has the right to access and disclose messages sent by employees. But there is no evidence that this uncertainty is chilling the use of electronic mail or that it cannot be dealt with adequately by giving higher levels of protection to any messages as to which the outcome is in doubt. Accordingly, no change in law was recommended by the task force.

Because ECPA is centrally concerned with protection against unreasonable searches and seizures by the government, because electronic mail usage in the workplace is growing rapidly, and because the statutory language now restricts disclosure only on public systems, there is some question whether the statute ought to be amended to provide greater protection of employee rights in the event that the government seeks access to electronic mail records. Right now, an employer whose electronic mail system is not offered to the public is not under an obligation even to inform the employee of the fact of a government inquiry. To be sure, there may be circumstances, such as those in which the employee is suspected of criminal action with an impact on the employer, where a requirement of notice would be inappropriate. And perhaps the government should in any event have the right to require nondisclosure in light of various showings, such as a substantial risk of destruction of evidence. Nevertheless, the group agreed that there may be some need for additional consideration of provisions that would require notice to employees, in some circumstances, when the government seeks access to contents of electronic mail sent or received by a particular employee.

This latter issue also relates closely to the question of whether current restrictions on the disposition of transactional records generated in the course of electronic communications are adequate, a subject deserving discussion in its own right.

Dossier building

In various contexts, members of the task force raised concerns about the proliferation of records automatically generated by electronic communications and electronically facilitated transactions. ECPA does not limit use and disclosure of such records, other than to the government. Such records, collected initially for legitimate reasons and lawfully possessed and used for various purposes, might nonetheless be used to compile detailed dossiers that, if published to third parties, could create a threat to privacy akin to that created by targeted surveillance coupled with invasive publicity.

The task force received an initial proposal for consideration of an amendment that would directly address the potential problem posed by such electronically generated dossiers. The task force did not, however, have enough time to consider thoroughly the complex issues that would be raised by any such proposal. Because the potential use of automatically generated electronic records to produce and publish unduly detailed data regarding the activities of an individual will likely remain a key privacy concern in the future, various members of the task force intend to continue to discuss proposals for dealing directly with this issue and may submit additional suggestions for consideration by the Judiciary Committee at a later time.

V. GOVERNMENT MONITORING

The task force reviewed a proposal currently pending before the Senate Judiciary Committee which directs electronic communications service and equipment providers to aid law enforcement officials in obtaining the plain text of voice or electronic communications where an appropriate warrant has been issued. The proposal is contained in two bills: S. 266, the Comprehensive Counter-Terrorism Act of 1991, and S. 618, the Violent Crime Control Act of 1991. It is stated as follows:

> It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text of contents of voice, data, and other communications when appropriately authorized by law.

The text of the resolution could be read to address three distinct issues or problems which could be faced by law enforcement officials in the future, as the network makes a transition from analog to digital transmission. First, digital transmission will make it easier for network service providers to enhance security and privacy by transmitting information with encryption, modulation, or other security enhancing features. Second, as the network goes digital and more information is switched in packets into a larger information stream, the ability to isolate individual communications at a central office switch becomes more technically challenging. Finally, the advent of powerful personal computers and off-the-shelf software gives the person originating the communication the ability to encrypt or otherwise enhance the privacy and security of a communication before it enters the network.

Based on discussions between Judiciary Committee staff and law enforcement officials, it appears that the intent of the resolution was to deal only with the first two issues, i.e. privacy and security features that are added by design features of the network. Addressing those narrow issues and seeking cooperation from service providers would be consistent with the current structure and text of ECPA which in 18 U.S.C. Sections 2511 and 2707 provides immunity for service providers, landlords, and others who comply with facially valid warrants by aiding law enforcement officials in conducting electronic surveillance. Clearly Congress contemplated and courts often direct communications service providers to provide technical assistance to law enforcement in placing taps. Stripping the encryption or security features which the service provider has added or helping law enforcement isolate a specific communication in the information stream would clearly be appropriate where a Title III warrant has been obtained.

The task force raised serious concerns, however, about several aspects of the drafting of the proposal. First, the proposal lacked a clear procedural standard that has always been present in any matter involving communications surveillance. Absent such a standard, specifying the circumstances when the service provider was required by law to assist the law enforcement agent, there is opportunity for misunderstanding, error, and abuse.

Second, the provision could discourage or effectively prohibit the use of privacy-enhancing features, such as cryptography. Such features are increasingly available with the widespread use of digitized transmission.

Third, there was no record established to support this change in current policy regarding Title III searches. Absent such a showing, the task force was unable to determine whether such a change was necessary at this time.

Finally, the task force recognized that there are specific areas of technological innovation that are important for communications privacy which require further discussion and evaluation. In particular, the task force recommended the examination of encryption technology and its potential impact on enhancing the privacy, security, and authenticity of electronic communications.

Conclusion: The task force felt that without a full record or understanding of the need for the proposed resolution, it could not make specific recommendations. The task force does urge the Judiciary Committee to establish a full record about the need for and impact of the resolution before consideration by the full Senate.

APPENDIX

MEMBERS OF THE PRIVACY AND TECHNOLOGY TASK FORCE

Chair: John D. Podesta, Esq., Podesta Associates, Inc.

Ms. Debra Berlyn, Executive Director, National Association of State Utility Consumer Advocates.

Mr. Jerry Berman, Information Technology Project of the American Civil Liberties Union.

Ms. Martina Bradford, Vice President, Government AT&T.

John J. Byrne, Esq., Federal Legislative Counsel, American Bankers Association.

Mr. Michael F. Cavanagh, Executive Director, Electronic Mail Association.

Mr. John Gilroy, Executive Director, Vermont Public Interest Research Group.

Jan-Lori Goldman, Esq., American Civil Liberties Union.

David Johnson, Esq., Wilmer, Cutler & Pickering.

Mr. Elliot Maxwell, Assistant Vice President for Policy and Issues Management, Pacific Telesis.

Mr. Thomas Mills, Director of Public Affairs, New England Telephone—Vermont.

Michael Nugent, Esq., Associate General Counsel and Vice President, Citicorp/Citibank.

Ronald Plesser, Esq., Piper & Marbury.

Marc Rotenberg, Esq., Computer Professionals for Social Responsibility.

Professor Glenn Smith, California Western School of Law.

Mr. James Sylvester, Director—Infrastructure Issues, Bell Atlantic.

Representative EDWARDS. Thank you very much, Mr. Berman.

There seems to be a discrepancy, Director Freeh, in the estimates as to future costs. Why is there a discrepancy? How do you respond to that?

Mr. FREEH. Again, not to fall back on the GAO report, but I think it is agreed and there is a consensus that without having even initiated either the standards-setting procedure or the engineering of that standards into telecommunications switching and other equipment, getting, as was pointed out, not just the carriers involved but the equipment manufacturers, I just think there is a very, very difficult block to fill with respect to estimating that cost.

We certainly know what the cost would be of not proceeding in terms of crime, destruction. I think the best and wisest way to approach it is how the bill now drafted approaches it, and that is to begin a standards-setting procedure, to have the industry design and upload the necessary software that is going to be required, and to address on a priority basis the things that most need to be done.

I wish I could give you an answer to that question. We know what it will cost not to do this, and if we make the decision that it is worth doing, which is certainly my recommendation, I think we proceed with a flexible-enough mechanisms, which are in the statute, for your oversight. If we reach a point where the cost estimates have been so far amiss by everyone involved, you can certainly intervene. The industry can intervene. A court can intervene. A district court judge could say that in his or her view, compliance is not necessary because the cost is not reasonable. I think there are a lot of mechanisms already built into that process.

Not knowing the exact cost cannot be a reason for not going forward.

Representative EDWARDS. Thank you.

Mr. Neel?

Mr. NEEL. Mr. Chairman, we may not be in great disagreement about this issue. Maybe we are simply not acknowledging the problem of making available massive amounts of money in the out years here, that is sort of the unstated problem.

You could ameliorate much of this by doing two things. First of all is lifting the cap on the time period after which you—at this point in the legislation, you don't provide for reimbursing for capability. As I said earlier, we don't know what kind of new technologies will need to be retrofitted or adapted, and that goes to the capability question. Those problems are not going to be solved in 4 to 6 years. Our sense is that it takes at least 5 to 6 years to simply develop a new product, so that cap on time would be a problem.

The second improvement would be to simply not require compliance, certainly not with penalties, huge financial penalties, if the Government is unable to reimburse. In other words, if you run out of money, if it turns out that in the first year you have to spend the whole $500 million and there is no more money authorized, that you then don't force with fines and other kinds of requirements including forcing a carrier to pull a service off, that you don't do that if a company can't be reimbursed.

Those would be significant improvements in terms of dealing with this cost problem.

Ms. EDWARDS. Mr. Chairman, to amplify on that a little bit, I would like to give reference to the points where we have identified opportunities to save dollars or to control the cost.

In the event that we move forward with the $500 million as the designated amount, the question becomes whether or not at the end of the designated period the law enforcement agencies are getting the kinds of capabilities that they need in a priority order, and that brings us to the point of prioritizing the specific needs, be it on the capacity or the capability side, and that prioritization would take place between the two parties, the law enforcement community and the industry. We think that that would be very important.

The second point I would like to emphasize is that on the cost containment side, there are solutions that are being developed today that will address some of these issues that we have talked about in general terms. It is important that those technical solutions are shared among the various participating members of the service providers so as not to spend a long period of time waiting for the solutions to transcend all of the carriers, but in addition to that, ultimately to save costs and prevent the redundant development of solutions.

So on the point of prioritizing, we think that is important for containing costs, but also sharing the technical solutions that are available today, those are important in the near term.

For the longer term, the point that Director Freeh raises in terms of setting standards and having those standards guide the development of new technologies I think is very important.

Representative EDWARDS. Mr. Wheeler?

Mr. WHEELER. Mr. Chairman, it is not surprising that nobody can put their hands around what the number is, because we don't know what the requirement is.

But there is a parallelism here in the two processes for capability and capacity, or rather, there should be a parallelism which doesn't exist. You look at the procedure the bill establishes for establishing capabilities. First of all, there is the working group which comes up with technical standards. Then there is a formal proceeding at the FCC, if necessary, to notice and comment on that.

On the other side of those items which are going to determine what the cost is, the capacity question, there is no such structure for debate, for exchange, for no, that doesn't make sense, let us do it this way, that kind of a thing. If there were in place a formal procedure, I think we would begin to get down to understanding what the requirements are and what is behind the requirements, and only then can we begin to understand what the costs are.

Representative EDWARDS. Senator Leahy?

Senator LEAHY. Thank you, Mr. Chairman.

Mr. Wheeler, just to follow up a little bit on this, you have expressed a concern that we don't know what the capacity is finally going to be, and I understand that. If the Attorney General has to pay for whatever capacity we use, won't that serve as a brake on shooting the moon on this issue?

Mr. WHEELER. I guess I wear two hats here, then, Senator. First of all, I will put on my hat as a taxpayer and say, I would like to see some constraints on what those numbers are.

Now let me put on my hat representing the industry and say that this bill doesn't step up and pay for whatever improvements there are. This bill says that you, the carrier, will spend the money to meet demands which the Government imposes on you. Then you will submit a bill to the Government for that, which we will reimburse you if they have the money.

Senator LEAHY. So what you are saying is the Government might still decide, maybe we need some capacity here. We haven't had any experience with it yet but we might, so let us require it and then see if we have the money to pay for it. Is that your concern?

Mr. WHEELER. Yes, sir.

Senator LEAHY. You don't think it would be the other way around?

Mr. WHEELER. I think one of the concerns is that nobody ever wants to get stuck with having said, we don't need that capacity in this place, because——

Senator LEAHY. And I share your concern there. I look at some of the experience we have had in these areas, particularly in the Department of Defense where you have to refine, refine, and refine something that you could have bought off the shelf for X-amount. But after you refine for every possible contingency, you do two things: It could cost 8–X instead of 1–X and be a good 10 to 15 years behind the curve.

I think of the example of deciding that we have to have nuclear bomb-proof fax machines and the Department of Defense went and developed and developed. As you know, fax machines have changed very rapidly in the last few years so now they have a lot of antiquated, huge, $40,000 fax machines which may survive a nuclear attack. You tend to wonder who is going to be sending faxes. Do you want to fax a press release, "we just got bombed."? [Laughter.]

Senator LEAHY. As somebody said, they could have just gone down to the local store and picked up a couple of extras, stuck them in a lead box and left them there just in case anybody is around to talk with afterwards. You would have had not only a more modern machine but you would have saved 80 percent of the cost. But I digress.

I am sorry, do you want to say something?

Mr. WHEELER. No, I think you don't digress. I think you are right on point. What is missing is that dialog, the, hey, wait a minute, do we really need a nuclear bomb-proof fax machine?

Senator LEAHY. Everybody uses poor Topsham Telephone Company. For those who don't understand, this has about 1,100 customers.

Mr. WHEELER. Five employees or something like that.

Senator LEAHY. Five employees, in a beautiful place in a State that I am despairing of ever seeing again if we don't get out of here. [Laughter.]

As much as I love Washington in August, I would much rather be in Vermont.

But the point is, I share a concern that I don't want somebody to say, "gee, just suppose the mafia chieftain decides to move up to Vermont." This is not, to anybody watching us on television, this is not an open invitation, we don't want him. [Laughter.]

But suppose he does. They had better be rewired up there just in case. We don't want to do that.

I think, though, in the testimony and the discussions I have had with the FBI and others, that there is a sense of reasonableness that we are trying to build into the legislation. I don't want somebody to build the bomb-proof fax machine. I don't want somebody to say, just because some criminal happened to vacation for one weekend in Vermont, they would have to be totally rewired and have two extra employees just in case. We don't want to do that.

Director Freeh, is this not a subject that you have looked at, the perfect being the enemy of the good in this whole thing?

Mr. FREEH. Just one response to that. Mr. Neel mentioned that the passage of the statute and the enactment of these mechanisms would be an invitation for the ubiquitous use, I think the word was, of wiretaps. I think that is just not valid.

Having been a prosecutor and a judge, knowing what is still going to be unchanged in terms of the legal requirements, I do not expect any additional wiretapping to be done because of any increased capacity. What may happen, and what has happened over 22 years, is an increase in the use of that technique because of the catastrophe of crime, particularly drugs and organized crime.

We have a pretty good idea, and this is why the cooperation, I think, is so critical, and it was alluded to by Mr. Neel, we have a pretty good idea where, based on past crime patterns, the most likely venues and the most critical needs for capacity are. We do not propose, and I don't think anybody is proposing, rewiring America on the bomb-proof fax machine theory. We will never, in any estimation of the use of this technique, require that type of ridiculous cost and preparation.

I think we know where the trends are showing the greatest difficulty. That is where the capacity has to be addressed first, as Ms.

Edwards mentioned, on a priority basis, to keep up with the people who are using telecommunications to commit more and more complicated crimes.

So I would take issue with the idea that this is going to spawn more wiretaps simply by the use of the capability and access and that I think we have a pretty good idea where we need to build to protect.

Senator LEAHY. Let me use an example on that. When you were a prosecutor, you were involved with the applications for wiretaps on occasions, is that correct?

Mr. FREEH. Yes, that is correct.

Senator LEAHY. As a Federal judge, you saw applications for wiretaps?

Mr. FREEH. Yes.

Senator LEAHY. Did you ever have an experience with a Federal judge that their first question about a wiretap was well, is it easy to do or not? Or rather, do they look at whether you have the probable cause, do you comply with the Constitution, do you follow the statute in applying for this?

Mr. FREEH. They certainly and very critically look at the probable cause. Perhaps more importantly, they look at the showing that is required to be made, which is that no other technique, including the most sophisticated, are amenable to getting the type of evidence which can be found by this technique applied very carefully.

The showing of necessity is almost as great as the probable cause showing, which is exactly what makes only less than 1,000 wiretaps per year and will be——

Senator LEAHY. In fact, that is my point. It is not like in some of the television shows where the sergeant turns and says, get a wiretap on this, and 2 minutes later somebody is listening in on something. It is a fairly cumbersome procedure. In fact, it is a very difficult and cumbersome procedure, is it not?

Mr. FREEH. That is exactly right. The more likely reaction, when the squad supervisor says, let us get a wiretap, everybody bails out of the squad area because of the work involved.

Senator LEAHY. I will put in the record the technology-based problems that are encountered by Federal, State, and local law enforcement agencies. There are 183 problems and how they are broken down.

Concerning the funds on this, will the administration be putting in line item requests for these funds? Do you know?

Mr. FREEH. I don't know the answer to that question. I know that the commitment is there and I know that the precise mechanisms, of course, need to be worked out between the Congress and the administration.

Senator LEAHY. Has any thought been given to burden sharing? Of the wiretaps, only about half are Federal, are they not?

Mr. FREEH. The majority are done by State and local authorities.

Senator LEAHY. That is what I thought. And yet this law, obviously, is going to have great benefit to them. In fact, if you, that is the FBI, develop techniques that work, I would assume that most State and local authorities, want to follow your techniques because you have done the research and development and everything else. Is there any possibility of having them share some of the costs?

Mr. FREEH. I think it would be very difficult. They certainly will pick up the costs of the lease-line, the implementation of the specific mechanisms to conduct the wiretap. But to burden, for example, the Petaluma Police Department and the county prosecutor for expenses which certainly would be amenable to solving the kidnapping and murder of Polly Klaus, for example, I think to put those kind of burdens on already pressed and overstrapped State and local authorities would probably be imprudent.

I think if you fix this for one, you fix it for all. Because there is such a great national and Federal interest here, both national security and criminal, it really does seem appropriate to me that the Federal Government bear the costs.

Mr. NEEL. Mr. Chairman?

Senator LEAHY. Yes?

Mr. NEEL. The Director suggested that I indicated that there would be wiretaps, that wiretaps would become ubiquitous. My comment, I think, was that the requirement that every telephone exchange in every rural area in upstate Vermont or wherever would be forced to build in the capability, whether there had ever been in history a request for a wiretap or, to use the director's analogy, might never be in the future, and that that would require those small rural exchanges to build in capability and incur those costs potentially nonreimbursed beyond the 4–6-year period built into this legislation.

If I might mention, the letter that Mr. Berman mentioned, if we could ask that this be put into the record from ten groups that have analyzed this legislation.

Senator LEAHY. It will be included.

I have a related question to ask both of you in this regard. Let us suppose we do appropriate $500 million. Director Freeh, you have testified that it could be more than that and it could be less than that. But suppose we do and we process with the Government paying for this. Let us assume we work out the formula that is realistic.

I would assume that the Government is first going to look to those places where the Director has said we know from historic investigations and law enforcement patterns that the need is greatest and they are more apt to have wiretaps. This is not going to be the Topsham Telephone Company in Vermont but it could well be in Manhattan or Dade County or other such places.

The money is expended there, and you go to the places that have been designated as the first priority, second, third, wherever it goes. But then you run out of money and you still have three or four priority areas, not the whole country but three or four other priority areas. Who pays? Do we stop? I am assuming the Congress says, we are up against our caps this year. There is no more money. Where do you go?

Mr. FREEH. My own view of that is that if this Congress, these committees made a finding that the cost/benefit of supplying further monies to a system which has been, perhaps, half-improved but not totally improved, if those fundings are no longer appropriate, then that money stops funding.

I would still be in a better place if I could have access to half of the criminal conversations than none of the criminal conversations.

I do fall back, however, on some of the arguments that Ms. Edwards suggests. I think over a long-term period, if the law enforcement standards can be incorporated into the industry standards and we are talking now about designing switches for 1998 and 1999, it seems to me that there will be a much more expansive benefit and a permeating benefit by starting early, particularly with the larger systems which will work to the benefit of upgrading the smaller systems.

Senator LEAHY. Without leaving a blueprint that might cause too much comfort to some, is it not safe to say that no matter what we do, there are going to be areas you are not going to be covering?

Mr. FREEH. That is correct. We have already made those choices with respect to private communications networks.

Senator LEAHY. This is the same thing in any kind of law enforcement. People, even under surveillance, people on some occasions escape surveillance or there is somebody else involved that law enforcement doesn't know about. We are not an Orwellian society where everyone is wired, is that not correct?

Mr. FREEH. That is absolutely correct. We never would have gotten John Gotti talking on a telephone, no matter what the access or capability was. There is a certain class of our targets, including spies, who are not going to be amenable to that. That doesn't mean that we give up the whole universe of opportunity.

Senator LEAHY. Mr. Neel, would it be the position of your organization that if the money stopped, then you are not prepared to say you would then take over the funding?

Mr. NEEL. We would hope not, because the burden would most likely fall on ordinary telephone rate payers. That is just the way the telephone company gets its money to do its work.

I think the problem here is, one, there is not a certainty of the continued flow of funds, but the other problem is that even though the money might cease under this legislation after 4 years or even under disputes of another kind, the requirement, we think, is still there. I would say that even though there may not be demands of every telephone company, the requirement to provide a capability to wiretap ordinary telephone conversations as well as these new enhanced services, call forwarding and so on, will still be there for every small telephone company.

The requirement for capability will be ubiquitous unless law enforcement, the Director has an idea of maybe carving out in advance the geographical areas that wouldn't be covered, and I don't think anybody would want to do that. That sort of prescribes the safe haven for criminals.

Senator LEAHY. We may increase the population in some of our rural towns unnecessarily.

Mr. NEEL. Your worst fear might become true under that scenario.

Senator LEAHY. Let us take these 183 cases. Were you unable to get wiretaps in all of those or were you just hindered in your wiretaps?

Mr. FREEH. We were hindered in carrying out the court orders, mostly the pen registers. That doesn't include many cases, not 183, but a few dozen cases where applications were not made for court-authorized wiretaps because of that deficiency.

Senator LEAHY. Ms. Edwards, what has GAO found? Have you found instances of inabilities to carry out court orders?

Ms. EDWARDS. We had discussions with members in the industry, both on the provider side and on the manufacturer side, and we also spoke with members in the law enforcement community. What we found was that there were reported instances where the law enforcement community had not asked for a particular tap to be made because they knew from prior conversations with industry representatives that it wasn't possible. So rather than going through the anxiety and the effort, as the Director pointed out, that is entailed in getting a court order to do the tap, they just chose not to go that route.

Senator LEAHY. In other words, they felt that if the capability had been there, they could have gotten the court order.

Ms. EDWARDS. They would have gotten a court order.

Senator LEAHY. But the capability wasn't there.

Ms. EDWARDS. That is right. That was from conversations. We did not identify particular instances, however.

Senator LEAHY. Under this legislation, and Mr. Neel, let me ask you about this, we say that the judge has to take into consideration the availability of funds in deciding whether to issue an enforcement order. Doesn't that protect you enough?

Mr. NEEL. We would hope so, but you have to understand that law enforcement is not your typical consumer. Telephone companies are essentially community-based corporations. No telephone company that I know of is going to want to deny law enforcement the opportunity to do its business, even if perhaps it doesn't have the money to pay for it or if it might be in question.

It would be better if the language of the legislation were more specific than just having the court taking into consideration the ability to pay. We would hope that the legislation would reflect more of a certainty that the Government will pay when the Government requests a product or service. It is a little like suggesting that if the highway patrol runs out of money in its budget and can't buy any more cars and radar detectors, that it shuts down the highway and no one can drive on the highway. It may be a little bit of hyperbole, but the law enforcement is not your typical consumer. No, that doesn't give us adequate comfort, but we think you could improve it in the legislation.

Senator LEAHY. My last question is would you agree, however, that if we do not make some changes as technology goes on, that a large part of law enforcement's capability to lawfully intercept conversations will be denied them?

Mr. NEEL. Two changes do need to be done. There needs to be a recommitment to the effort of Government and the private sector to work out standard problems. That is going to be required whether you pass the legislation or not. You can't just wave a magic wand and declare that this will be done. Government and industry are going to have to work those things out.

Second, you have to make it possible to pay for it. If you can do that, then this can be a reality and you can solve law enforcement problems and protect consumers.

Senator LEAHY. But my point still remains, utilizing today's technologies for wiretapping, are we not fast approaching the time, just using today's technology, when a great deal of the ability of law enforcement, will be denied them?

Mr. NEEL. In a number of cases with new enhanced services, that is probably true.

Senator LEAHY. Thank you.

Director Freeh, that is definitely your position?

Mr. FREEH. Yes, that is my position.

Senator LEAHY. Thank you, Mr. Chairman.

Representative EDWARDS. We welcome the Senator from South Dakota, Mr. Larry Pressler.

Senator PRESSLER. Have my colleagues had a chance to inquire? I am the last to arrive, so I want to be the last to ask. Why don't you go first.

Representative EDWARDS. Mr. Coble?

Representative COBLE. Thank you, Mr. Chairman. Thank you, Senator Pressler.

Mr. Chairman, I will be short and sweet. I apologize that I had to be away on the floor. Prior to my question, lady and gentlemen, I want to reiterate what I said were two significant goals at the outset, to assure law enforcement that it does not lose its capability on the one hand and to assure furthermore that individual private rights are not trashed and summarily dismissed.

I believe each of these goals is laudable and I believe each of these goals is realistic if a proper balance is struck. I think balance is the key word here.

Having said that, Mr. Director, let me put the question to you, and any of you feel free to answer. I want to admit to you that although I am not computer illiterate, neither am I computer competent, so I am about to steam in computerized waters that are always invested with rocks, shoals, and reefs for me because of lack of information computerwise.

Scope of coverage, Mr. Director, I think is an important issue to the topic at hand. Under the term "common carrier", this bill covers local exchange carriers, long-distance carriers, competitive access providers, cellular companies, and cable companies when they offer telephone service. Not included in the scope, as you all know, are all computerized systems, that is commercial Internet, some computer networks, pure computer networks, I suppose.

Having said that, I can visualize the mafia kingpin who is considering relocating in Vermont, to use the Senator's term. [Laughter.]

Senator LEAHY. I am just afraid somebody is going to be encouraged. We don't want them.

Representative COBLE. Senator, I wanted to stay in the New England area, not in the Southeast. [Laughter.]

Representative COBLE. But I see this guy locating wherever—we will even say South Dakota, Larry—[Laughter.]

But when he is going to relocate, I fear, lady and gentlemen, that he may detect an alternate highway. Oh my gosh, he says, these matters are not included in the scope so I will do my communicating here and there and yonder.

Am I reasonably on course, Director? Let me hear from you.

Mr. FREEH. Yes, I think you are directly on course. There is always going to be and perhaps increasing because of the technology developments, a range of criminal activity and a particular type of criminal actor who will be immune from the best-designed and best-built system. There are other tradeoffs, however. In the event that we are unable to use telephone electronic surveillance, we do have under the statute the authority to approve a court-authorized microphone surveillance. There is new technology that is coming which will even enhance the ability to use microphone surveillance as opposed to telephone surveillance.

There is a part of the sophisticated criminal world which will not be captured in this bill, but it is not captured now. We now have a very small and expert group of spies, terrorists, organized criminals who have their own encryption devices, who are immune from the type of electronic surveillance that the overwhelming majority of our subjects are not, kidnappers. Most of the wiretaps that State and local authorities use are in kidnapping and extortion-type cases. In drug cases, most of the actors are sophisticated people who use phone beepers and telephones to conduct their business.

So you are absolutely right. We are missing a part of the playing field, but our position is we don't want to miss the whole playing field.

Representative COBLE. Thank you. Is there anybody else who wants to be heard on that? I think that is a good answer, Mr. Director.

[No response.]

Representative COBLE. Mr. Chairman, I will conclude. You will recall in my opening statement that I expressed concern about the cost. Upon my return, I see others on the panel here share my concern about that.

I can just see, folks, a common carrier having relied upon the assurance that this is going to cost $500 million and dust starts flying and they start making all sorts of sophisticated improvements and submit their bill up here on the Hill. Oh, I am sorry, Mr. Carrier, the bucket is dry, the well has gone dry. There is no more money. I think that is something we must address before the fact rather than after the fact.

Yes, sir, Jerry?

Mr. BERMAN. At the end of the drafting process, language was added to the legislation which says that lack of appropriated funds, and I think Mr. Neel was referring to it, could be a consideration in whether compliance with the requirements are reasonable.

It would be interesting to hear the Director, because he seemed to be suggesting that it was more than a consideration, that if the requirements could not be met with appropriated funds, he would still say, well, I have half of the network taken care of and that is better than having none of the network taken care of. Perhaps he was suggesting that it would be more than a consideration. It might be a defense or at least a limitation on meeting those requirements if there are no funds. Then that requires prioritizing within the system, and then it says to Congress, if you want compliance, you have to appropriate more funds.

Mr. FREEH. I think the interested parties are completely protected. I cannot conceive of—I shouldn't say this. I think it would be unlikely, extremely unlikely for a district court judge in the process which is contemplated by this legislation to force compliance or use any sanctions when compliance is impossible because of the nonreimbursement which is the predicate in the legislation. I can't think of a better protection than that and a better definition of reasonableness.

For district courts who err, of course we have courts of appeals. So I don't think it is a dangerous path for the parties to begin to tread.

Mr. WHEELER. Mr. Director, with all due respect, there are two issues here. One is the issue of a defense in court against an action. The other is a requirement. We don't want to get to court. We don't want to have to say, hey, but—if the law says you are going to provide this capability and this capacity, we want to salute the flag and say, yes, sir, we will. Then we write the check and we turn around and, to use your term, the bucket is dry.

Mr. FREEH. I guess I can't allay all of that anxiety. What I will say, for instance, is with respect to the 183 instances that we have documented where the execution of court orders have been frustrated, in none of those instances was any action undertaken or, as far as I know, contemplated by the Government authorities to force compliance.

Your industries, all of your industries represented here, are our natural and historical allies and colleagues in this endeavor. We have never had an adversarial relationship with any common carrier. I did hundreds of court-authorized wiretaps in the Southern District of New York as a prosecutor. I never heard of a challenge where a prosecutor decided to force compliance under the current statute, which because of the general language of "all necessary assistance" would certainly give jurisdiction for the Government to come into court.

We have never done that. I don't contemplate that would ever be done, because the whole premise of this regime, in order to work, is a cooperative effort where the parties are melding standards and not in an adversary proceeding.

So I think the rule of reasonableness protects you and I think the track record and the history here should assure you that you will be well protected.

Representative COBLE. Mr. Chairman, I told you I would be short and sweet, so before I become long and sour, I will yield back the balance of my time.

Representative EDWARDS. Thank you.

Senator Pressler?

STATEMENT OF HON. LARRY PRESSLER, A U.S. SENATOR FROM THE STATE OF SOUTH DAKOTA

Senator PRESSLER. Thank you, Mr. Chairman, for holding this hearing. I think it is very important.

Let me ask from a layman's point of view what this really means in terms of the new so-called information superhighway, or whatever that means to other people. Just this morning, the Senate Commerce Committee passed out a huge infrastructure bill, which I believe the House has already passed, which will now go to the Senate floor. But are we talking about communications between would-be criminals that could pass not through a telephone but through portions of the information superhighway and what might those parts of the information superhighway be? How does this legislation or this discussion apply to that?

Mr. FREEH. Senator, if I may, first, I think it is an excellent question. It is a discussion I had with the Vice President when he raised it.

In the simplest layman's terms, my answer, and I am not a technical person, is that as much as we need and want a superhighway of information, most reasonable people would agree that we need a policeman on that highway to protect the citizens who use it.

We are talking about, in this bill as proposed, a telecommunications utilized, transited, facilitated by a common carrier, whether it go from a computer to a computer via a common carrier network or directly between common carriers and switching points. We have exempted, as we have discussed, a segment, a fairly significant segment, of the evolving telecommunications industry. We are really talking about phone-to-phone conversations which travel over a telecommunications network in whole or part. That is the arena of criminal opportunity that we are discussing.

Senator PRESSLER. What other portions of the information superhighway could people communicate with the new technology that there is not now a means of listening in or following?

Mr. FREEH. From what I understand, and again, I am probably the worst person in this room to answer the question, communications between private computers, PC–PC communications, not utilizing a telecommunications common net, would be one vast arena, the Internet system, many of the private communications systems which are evolving. Those we are not going to be on by the design of this legislation.

Senator PRESSLER. Are you seeking to be able to access those communications also in some other legislation?

Mr. FREEH. No, we are not. We are satisfied with this bill. I think it delimits the most important area and also makes for the consensus, which I think it pretty much has at this point.

Senator PRESSLER. Yes, but in the future, will you be seeking the ability to tap into those other forms of communication?

Mr. FREEH. It is certainly a possibility. I am sure if, God forbid, somebody blows up the World Trade Center 10 years from now using a PC–PC private communications network, a question would validly be raised in the Congress and by the President as to whether that form of communication now needs to be accessed. But we are not taking that position now. We are not contemplating coming back and asking for additional coverage.

Senator PRESSLER. So what we are looking for is strictly telephone, what is said over a telephone?

Mr. FREEH. That is the way I understand it, yes, sir.

Senator PRESSLER. That runs through a digital—yes, go ahead.

Mr. BERMAN. My understanding is, I think, a little different, which is that the Internet providers are not covered under this, but the Internet traverses the public switch telephone network. It uses the transmission and switching facilities of the networks that are covered under this legislation.

My understanding is that that communications stream has to be delivered into the future by common carriers and therefore a communication that is travelling across the Internet which is the subject of a court-ordered wiretap would be intercepted. PBX's are not covered under the statute, but the FBI's technical experts have said that if they get handed the PBX, in other words, they could get the wiretap at the hotel, that they have ways of getting that communication without requiring all PBX designers to re-engineer their networks.

So I think that for the foreseeable future, the world of telephone communications and even data communications where people are using a ubiquitous network, and even when that is partly the cable network, that law enforcement needs are going to be met.

But at the same time, what is left out is a totally ubiquitous or penetrating FBI compliance which will require every piece of every network to design to meet this requirement because actually, it is not necessary.

Senator PRESSLER. Each Senator, and I suppose each member of the House, has a special telephone in our office that supposedly has a secure line. I guess when the Secretary of State wants to tell us a secret, they can call us up and tell us or something like that.

Does that go through a digital capacity, or how does that get scrambled? Does anybody know? How does that work?

Senator LEAHY. It is just a regular telephone but it has an algorithm built into it. What you do is you identify yourself with your key when you put it in and you can take the secure phone anywhere. You can take the secure phone home and plug it into your house and make a telephone call over your regular house line.

Senator PRESSLER. Can you now tap into that? Do you have the capability?

Senator LEAHY. You can tap into the line. Then you have to be able to decipher what it says.

Senator PRESSLER. Does that become a digital thing on the line?

Representative COBLE. It is not a digital——

Senator LEAHY. It is entirely different. You are dealing with apples and oranges. It doesn't make any difference whether it is digital or otherwise. It is a question of whether you have the algorithms to decipher it. Now you are going into another issue which we don't want to go into and won't go into.

Senator PRESSLER. Would you be opposed to requiring the FBI to meet a heightened standard for such content information, perhaps somewhere between probable cause and a reasonable suspicion? For this additional ability to listen in, would the standard be the same for a warrant? What standard would you want to use, probable cause or reasonable suspicion?

Mr. FREEH. The current standards are unchanged under the statute. We would still need, for contents of conversations, the probable cause standard, which is the standard for a search warrant for an indictment.

Senator PRESSLER. In what types of crimes is electronic surveillance most critical for prosecution?

Mr. FREEH. It is most critical with respect to organized crime, drug trafficking, and terrorism on the Federal level. On the local level, it is more in the realm of kidnapping and extortion cases.

Senator PRESSLER. I may have some additional questions for the record. I thank you very much.

Representative EDWARDS. We thank all the witnesses. We will have some more questions. I am sure the witnesses will cooperate in responding promptly.

I would like to insert a written statement from the AT&T Corporation into the record.

I think we had a very useful hearing. We thank you for your cooperation, and we are adjourned.

Senator LEAHY. Thank you, Mr. Chairman.

[Whereupon, at 2:54 p.m., the subcommittees were adjourned.]

APPENDIX

ADDITIONAL SUBMISSIONS FOR THE RECORD

CPSR WASHINGTON OFFICE,
Washington, DC, January 24, 1994.

The PRESIDENT,
The White House,
Washington, DC.

DEAR MR. PRESIDENT: We are writing to you regarding the "Clipper" escrowed encryption proposal now under consideration by the White House. We wish to express our concern about this plan and similartechnical standards that may be proposed for the nation's communications infrastructure.

The current proposal was developed in secret by federal agencies primarily concerned about electronic surveillance, not privacy protection. Critical aspects of the plan remain classified and thus beyond public review.

The private sector and the public have expressed nearly unanimous opposition to Clipper. In the formal request for comments conducted by the Department of Commerce last year, less than a handful of respondents supported the plan. Several hundred opposed it.

If the plan goes forward, commercial firms that hope to develop new products will face extensive government obstacles. Cryptographers who wish to develop new privacy enhancing technologies will be discouraged. Citizens who anticipate that the progress of technology will enhance personal privacy will find their expectations unfulfilled.

Some have proposed that Clipper be adopted on a voluntary basis and suggest that other technical approaches will remain viable. The government, however, exerts enormous influence in the marketplace, and the likelihood that competing standards would survive is small. Few in the user community believe that the proposal would be truly voluntary.

The Clipper proposal should not be adopted. We believe that if this proposal and the associated standards go forward, even on voluntary basis, privacy protection will be diminished, innovation will be slowed, governmentaccountability will be lessened, and the openness necessary to ensure the successful development of the nation's communications infrastructure will be threatened.

We respectfully ask the White House to withdraw the Clipper proposal.

Sincerely,

PUBLIC INTEREST CIVIL LIBERTIES ORGANIZATIONS,

MARC ROTENBERG,
CPSR,

CONRAD MARTIN,
Fund for Constitutional Government,

WILLIAM CAMING,
Privacy Consultant,

SIMON DAVIES,
Privacy International,

EVAN HENDRICKS,
US Privacy Council,

SIMONA NASS,
Society for Electronic Access,

ROBERT ELLIS SMITH,
Privacy Journal,

JERRY BERMAN,
Electronic Frontier Foundation,

CRYPTOGRAPHERS AND SECURITY EXPERTS,

BOB BALES,
National Computer Security Association,

JIM BIDZOS,
RSA Data Security Inc.,

G. ROBERT BLAKLEY,
Texas A&M University,

STEPHEN BRYEN,
Secured Communications Technologies, Inc.,

DAVID CHAUM,
Digicash,

GEORGE DAVIDA,
University of Wisconsin,

WHITFIELD DIFFIE,
Sun Microsystems,

MARTIN HELLMAN,
Stanford University,

INGEMARSSON INGEMARSSON,
Universitetet i Linkvping,

RALPH C. MERKLE,
Xerox PARC,

WILLIAM HUGH MURRAY,
Security Consultant,

PETER G. NEUMANN,
SRI International,

BART PRENEEL,
Katolieke Universiteit,

RONALD RIVEST,
MIT

BRUCE SCHNEIER,
Applied Cryptography (1993),

WINN SCHWARTAU,
InterPact,

RICHARD SCHROEPPEL,
University of Arizona,

STEPHEN WALKER,
Trusted Information Systems,

PHILIP ZIMMERMANN,
Boulder Software Engineering,

INDUSTRY AND ACADEMIA,

ANDREW SCOTT BEALS,
Telebit International,

MIKKI BARRY,
InterCon Systems Corporation,

DAVID BELLIN,
North Carolina A&T University,

MARGARET CHON,
Syracuse University College of Law,

LAURA FILLMORE,
Online Bookstore,

SCOTT FRITCHIE,
Twin-cities Free Net,

ROB KLING,
University of California, Irvine,

GARY MARX,
University of Colorado,

RONALD B. NATALIE, JR.,
Sensor Systems Inc.,

HAROLD JOSEPH HIGHLAND,
Computers & Security,

DOUG HUMPHREY,
Digital Express Group, Inc.,

CARL POMERANCE,
University of Georgia,

ERIC ROBERTS,
Stanford University,

JONATHAN ROSENOER,
CyberLaw & CyberLex,

ALEXIS ROSEN,
Public Access Networks Corp.,

STEVEN ZORN,
Pace University Law School.

MATT L. RODRIGUEZ,
SUPERINTENDENT OF POLICE,
Major Cities Chiefs, March 16, 1994.

Hon. PATRICK J. LEAHY,
Subcommittee on Technology and the Law,
U.S. Senate, Washington, DC.

For years, court-authorized electronic surveillance has been one of law enforcement's most potent weapons against drug traffickers, organized crime figures, terrorists other offenders. Now, with the emergence of digital telephony, this tool is being seriously threatened.

As you may know, digitally coded communications are extremely difficult to intercept with existing technology. Despite this limitation, the telecommunications industry remains unwilling to invest in the necessary software that would allow police agencies to conduct wiretaps of digital communications. As this new technology becomes more commonplace, law effectiveness—and, ultimately, the safety of the public—will be jeopardized something is not done and done quickly.

The Major Cities Chiefs Association, a professional organization of police executives representing the 49 largest metropolitan areas in the United States and Canada, is extremely concerned with this situation. Onbehalf of our membership, I am writing to urge Congress to pass appropriate legislation that would ensure law enforcement agencies the ability to conduct court-authorized electronic surveillance in conjunction with digital telephony.

The FBI and other federal agencies have taken the lead in advocating such legislation in recent years, because electronic surveillance is so important to their investigatory and enforcement activities. Wiretaps were instrumental in the identification, apprehension and prosecution of the terrorists recently convicted in the World Trade Center bombings.

But electronic surveillance is a critical tool for local law enforcement agencies as well. Most wiretaps are conducted at the local level, targeting serious problems of crime, violence and drug abuse in our neighborhoods. In cities across the country, thousands of dangerous offenders have been apprehended and enormous quantities of illegal drugs and firearms have been seized as a direct result of court-authorized wiretaps.

Two years ago, for example, Chicago police relied heavily on electronic surveillance to break up a major drug trafficking ring on the City's South Side. Operation Englewood resulted in the indictment of eight high-level dealers (including a major supplier who lived outside the neighborhood), the seizure of significant quantities of cocaine, and the forfeiture of 12 pieces of real estate, five businesses, 25 vehicles and an airplane. More importantly, the mission dealt such a severe blow to drug-dealing operations in this traditionally high-crime neighborhood that activity has never returned to its former pace.

Our success in this and countless other operations would have been impossible without the availability of court-authorized wiretaps. In complex cases where infiltration of criminal enterprises is so crucial, information simply cannot be obtained by any other method than electronic surveillance. And without information, law enforcement will never be able to build the cases that have a lasting impact on drug trafficking, domestic terrorism, extortion and other forms of serious, violent crime.

What law enforcement is seeking is nothing more than a continuation of the closely monitored and well regulated electronic surveillance capability we have used in the past. We are not looking to expand our authority in this area. The Major Cities Chiefs and other law enforcement professionals recognize the personal privacy rights of our citizens, and we understand and support the need for strong judicial oversight of the use of wiretaps. We are merely trying to ensure a level playing field for the future.

The situation is urgent. The federal government has been trying for four years to obtain the cooperation of the telecommunications industry, without positive results. We cannot wait any longer. Digital telephony is expanding so rapidly that without immediate research and development of compatible electronic surveillance software, effective law enforcement at the local level, not to mention national security, will be threatened.

The Major Cities Chiefs Association urges you and your colleagues to support legislation that ensures law enforcement agencies will continue to have the electronic surveillance tools that we have used so judiciously and successfully in the past.

Sincerely,

MATT L. RODRIGUEZ,
Superintendent of Police,
Chicago Police Department.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE,
Alexandria, VA, March 17, 1994.

Hon. DON EDWARDS,
Subcommittee on Civil and Constitutional Rights,
Washington, DC.

DEAR CHAIRMAN EDWARDS: While the International Association of Chiefs of Police was not asked to testify at the March 18 Senate Subcommittee on Technology and the Law/House Subcommittee on Civil and Constitutional Rights joint hearing on Digital Telephony, we stand in strong support of the FBI position on this issue which will be offered in Director Freeh's testimony.

Recently, I was disturbed to find an article on this issue—law enforcement's ability to conduct wiretaps—on the Business page of the *Washington Post* March 12, 1994 edition. The article should have appeared on the front page as a national security and public safety issue.

Apparently a telephone and computer business coalition objects to the idea of assisting law enforcement in its efforts to protect the public from terrorists, drug dealers and organized crime activities.

The big companies are resisting cooperation on this issue ostensibly in order to promote public confidence in the privacy of new communication technologies. The facts are that these companies would have to go to additional expense in designing their new technologies, which they are unwilling to do.

The new digital technology greatly enhances telecommunications, but it renders obsolete the ability of law enforcement to implement court ordered wiretaps. Law enforcement rarely conducts wiretaps in this country, and when they are done, it is with the approval of a judge who has reviewed a detailed request. To wiretap without such prior approval is illegal, and any information obtained from an illegal tap is inadmissible.

No one is asking for more authority to conduct wiretaps—just the ability to perform the ones that are authorized. These telecommunications company executives should be working with FBI Director Louis Freeh to solve a very serious problem rather than writing him memos about how their businesses could be impacted.

These executives should be willing to make the same investment in public safety and crime prevention as they do in their telecommunications equipment.

Let's not afford criminals additional opportunities to conduct illegal activity unfettered by law enforcement. The next time we experience terrorist activity like the death and destruction at the World Trade Center or the attempted bombing of the tunnels in New York, who should we call when an authorized wiretap cannot be executed—the phone company?

The IACP and its many thousands of members nationwide urge you to examine this issue from the perspective of its critical relevance to public safety and adopt law enforcement's position regarding digital telephony.

Sincerely,

CHIEF, SYLVESTER DAUGHTRY, JR.,
President.

OPASTCO,
Washington, DC, September 22, 1994.

Hon. DON EDWARDS,
U.S. House of Representatives,
Washington, DC.

DEAR CONGRESSMAN: The Organization for the Protection and Advancement of Small Telephone Companies (OPASTCO) is writing to express some of the concerns that it has with H.R. 4922. This legislation, which clarifies a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, presents some serious issues for local exchange carriers, especially those that serve rural areas.

OPASTCO is a national trade association of more than 445 independently owned and operated telephone companies serving rural areas of the United States and Canada. Its members, which include both commercial companies and cooperatives, together serve over two million customers. OPASTCO is concerned about the effects that some of the requirements of this legislation will have on its members and their customers.

First and foremost, OPASTCO questions the necessity of this legislation. According to the testimony of Roy Neel, president of the United States Telephone Association, a survey of FBI offices indicates that FBI agents have not encountered any technology-based problems in conducting wiretaps in recent years. Furthermore, it appears that the biggest problem may be the capacity limitations in the wireless and cellular environment. Thus, it does not necessarily follow that the solution to that problem must include provisions that may require a (local exchange carrier) LEC to upgrade its network before it is appropriate.

In addition to the fact that this legislation is probably unnecessary, it imposes unwarranted burdens on LECs. One such burden is increased costs. These extra costs will be particularly burdensome for small and rural LECs. This legislation also does not have sufficient protection against government requirements that may be unreasonable. The scope of the coverage also raises some problems. These are a few of the provisions that create the greatest concern for the small LEC industry.

Satisfying the requirements of this legislation will be costly to small and rural LECs. The FBI indicates that the cost to accommodate these provisions is approximately $500 million. Other sources indicate that this estimate is woefully short of the true cost to the industry. Thus, who will cover these costs if the FBI's estimates are inadequate? The logical assumption is that it will be the carriers' responsibility, and ultimately that of the ratepayer.

Many small and rural LECs would face severe hardship in order to comply with the requirements of this legislative proposal. Their ability to raise the necessary capital to satisfy the requirements of this legislation is circumscribed by the fact that they serve low density, high cost areas. It is imperative that this legislation ensures that LECs are compensated for complying with this legislation.

OPASTCO believes that there should be some reasonable restrictions placed on the government's access to information. OPASTCO is concerned that, without limitations, the government's requests of the LECs may increase dramatically. For example, the Drug Enforcement Agency recently requested that a LEC supply the "identity of published and unlisted residential and business telephone * * * by area code, and telephone number, together with first name, last name (company name), address, city and state for all published and unlisted residential and business telephones in the service area * * *." Such a request is excessive. And without limitations, there is no reason to believe that these excessive, and expensive requests will not continue unabated. One way to solve this problem is to require the government to establish priorities and budget for its requests. This would limit requests to those that are reasonable. Moreover, it would enable the government to compensate carriers for satisfying those requests.

This legislation covers only a portion of the telecommunications traffic. Only those communications that are carried on the public switched network will be accessible to law enforcement officials under this legislation. Private networks are not subject to the requirements of this legislation. Thus, if users find a way to divert their traffic to the "secure" private network, then the effort and cost of making the public network accessible to law enforcement officials will have been all for naught. Additionally, this potential loss of users from the public switched network to the more secure private network may impede the development of the national information infrastructure.

OPASTCO believes that this far-reaching legislation is not necessary. Notwithstanding that position, OPASTCO believes that Congress is intent upon its passage. The ramifications of this legislation are great and OPASTCO has many concerns that transcend the scope of this letter. However, these are the most pressing issues for small LECs. OPASTCO urges Congress to address at least these issues as it contemplates this legislation.

Sincerely,

JOHN N. ROSE,
Executive Vice President.

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL,
Washington, DC, March 17, 1994.

Hon. PATRICK J. LEAHY,
Subcommittee on Technology and the Law,
U.S. Senate, Washington, DC.

Hon. DON EDWARDS,
Subcommittee on Civil and Constitutional Rights,
U.S. House of Representatives, Washington, DC.

DEAR CHAIRMAN LEAHY AND CHAIRMAN EDWARDS: The purpose of this letter is to express the support of the National Association of Attorneys General (NAAG) for legislation that would clarify the responsibility of the telecommunications industry to continue to assist law enforcement with court-authorized electronic surveillance despite advancing technologies. In 1992, the Association adopted a resolution supporting such legislation. The resolution is attached hereto. We understand that you will hold a joint hearing on March 18, 1994 with respect to this matter, and we respectfully request that this letter and the attached resolution be made a part of the hearing record.

The court-authorized interception of certain targeted communications is crucial to law enforcement's ability to investigate and prosecute individuals involved in criminal conduct. The lawful efforts of state and local law enforcement agencies in conducting court-authorized wiretaps has been threatened by the introduction of advanced technologies, including digital telephony, which facilitate transmission of multiple commingled communications and thus render law enforcement incapable of intercepting specific communications to the exclusion of all others. These new technologies must therefore be modified if law enforcement is to remain capable of using the highly effective tool of electronic surveillance.

Significantly, NAAG does not seek an expansion of the authority of law enforcement to conduct court-authorized electronic surveillance, nor does NAAG seek streamlining of the procedures that must be undertaken to conduct such surveillance. Rather, state and local law enforcement seeks only to preserve the ability to do that which they already have the authority to do pursuant to federal and state statutes.

Federal law requires the telecommunications industry to provide law enforcement with "all information, facilities, and technical assistance necessary to accomplish the interception." 18 U.S.C. §2518(4) and 3124(a)(b). The National Association of Attorneys General urges the clarification of this responsibility, as it relates to new and advanced technologies, through the passage of federal legislation requiring telecommunications providers, when authorized by law, to provide law enforcement with the capability of intercepting targeted communications of persons engaged in criminal conduct, to the exclusion of all other communications.

The Association appreciates your consideration of this issue which is so important for law enforcement.

Sincerely,

HUBERT H. HUMPHREY III,
President,
Attorney General of Minnesota, National Association of Attorneys General.

COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY,
Washington, DC, March 18, 1994.

Hon. PATRICK J. LEAHY,
Subcommittee on Technology and Law,
U.S. Senate, Washington, DC.

Congressman DON EDWARDS,
Subcommittee on Civil and Constitutional Rights,
U.S. House Office Building, Washington, DC.

DEAR SENATOR LEAHY AND CONGRESSMAN EDWARDS: I am writing to you on behalf of CPSR to express our support for your public hearings on the FBI Digital Telephony plan and the Clipper Chip. Both proposals raise long-term concerns about the future of communications privacy in the United States.

CPSR has a particular interest in these matters. As an organization of professionals in the computing field, we have a long-standing concern that new technologies be designed to provide strong privacy protection for networkusers. Privacy protection is a necessary condition for the successful deployment of advanced network technologies. Proposals that limit privacy protection will ultimately slow the development of advanced networks.

In late January we sent a letter to the White House, signed by many of the most distinguished cryptographers in the United States, asking that the Clipper proposal be withdrawn. (See attached). In the past month nearly 50,000 network users have added their names to that letter. If more people understood the implications of the Clipper plan, the number could easily be 500,000.

During the last-several years, we have also conducted extensive Freedom of Information Act litigation regarding the Clipper proposal and the Digital Telephony proposal. Documents disclosed as a result of our FOIA litigation have raised Directors substantial doubts about some of the claims made by the government in support of these initiatives.

This letter highlights our findings.

The Clipper proposal

- The National Security Agency usurped the authority of the Department of Commerce and violated the Computer Security Act of 1987 in the development of the Clipper plan. The original Commerce Department plan to develop open, unclassified standards for public key cryptography was revised by the National Security Agency. The NSA substituted a hardware-based, classified standard o that certain surveillance features could be incorporated (*CPSR* v. *National Institute of Standards and Technology,* No. 92–0972, D.D.C.)
- The National Security Agency, not the National Institute of Standards and Technology, has dominated the process of developing security standards for civilian communications.
- A related technical standard for "digital signatures" was purposefully designed by the NSA to minimize its privacy capabilities.
- The FBI and the NSA worked jointly on the development of the Clipper proposal and the Digital Telephony plan (*CPSR* v. *FBI,* 92–2117, D.D.C.)
- Many of these problems with the development of technical standards arose because a national security directive issued by President Bush bolstered the authority of the NSA at the expense of the Department of Commerce (*CPSR* v. *Department of Defense and National Security Council,* No. 91–13.)

A good deal of relevant information continues to be withheld by the government.

The Digital Telephony proposal

- The General Services Administration and the National Telecommunications and Information Administration both opposed an earlier version of the Digital Telephony plan and cited potential threats to national security if the proposal went forward.

- None of the FBI field offices has yet documented an instance where a lawful intercept was frustrated as a result of advances in digital technology. (*CPSR* v. *FBI,* 92–2117, D.D.C.)
- As early as 1992, the FBI anticipated that private communications firms would strongly oppose the legislative proposal.
- The plan to make the network easier to wiretap was code-named "Operation Root Canal"

The FBI also classified certain portions of the 1992 GAO assessment of the Digital Telephony proposal, thus keeping relevant information about the potential problems with the proposal from the public.

Assessment

The Clipper proposal resulted from the National Security Agency's desire to develop surveillance standards for US communications networks. Clipper was not developed by the agency charged with developing technical standards, nor do network user support the standard.

The Digital Telephony proposal is based on the suspect premise that new technologies have hindered the ability of law enforcement to conduct criminal investigations. In fact, new technologies have clearly expanded the ability of law enforcement to monitor individuals, to gather personal data, and to obtain transactional records generated by telephone communications.

The real challenge facing the Judiciary Committees is to narrow the scope, not expand, of the permissible seizure of personal information generated by advanced communications networks. In particular:

1) Amendments to the ECPA should narrow the use of subpoenas to obtain telephone toll records. The increasing use of subpoenas combined with the growth of digital networks has increased dramatically the amount of information available to law enforcement that does not require a judicial warrant. This trend runs contrary to the spirit of the federal wiretap statute and should be reversed.
2) Amendments to the ECPA should require annual reporting requirements that detail the number of requests for telephone toll records, telephone lines covered, and records obtained. Similar reporting requirements currently exist for wiretap and pen register warrants.
3) A privacy agency should be established within the federal government. Such an agency could help ensure that proposals such as the Digital Telephony proposal are not put forward without a proper review by an agency competent to evaluate the implications of such a plan.

Though some have described encryption as a form of "societal paranoia," there can be no doubt that encryption is the single most important technology for the protection of communications privacy. Not only does encryption provide for the confidential transmission of electronic communications, it also permits the authentication of business documents, and provides the basis for new forms of private communications. Policies that restrict the development of encryption or expand the ability of law enforcement to gather personal data will reduce privacy protection and diminish the value of communication networks in the United States.

We appreciate your consideration of our views. We would be pleased to provide to you or your staffs whatever additional information you request.

Sincerely yours,

MARC ROTENBERG,
Director.

DAVID SOBEL,
Legal Counsel.

District Attorney's Office,
Philadelphia, PA, March 28, 1994.

Hon. Patrick J. Leahy,
Subcommittee on Technology and the Law,
U.S. Senate, Washington, DC.

Hon. Don Edwards,
Subcommittee on Civil and Constitutional Rights,
U.S. House, Washington, DC.

Dear Senator Leahy and Congressman Edwards: In response to the NDAA memorandum from Jim Polley inquiring about law enforcement's concern as it relates to digital telephony, I offer the following:

In the Fall of 1991, this office was involved in an investigation which involved the extensive use of cellular telephones by the targets. One of the features being offered by the cellular industry is called "Follow Me Roaming". This feature allows a cellular telephone, operating out of its home switch to have all incoming calls automatically forwarded to it no matter where in the country it is operating. If a court authorized intercept is being conducted on this particular instrument, it would appear to be inactive to us but could still be making and receiving calls. This occurs because once "Follow Me Roaming" is activated, the cellular system, which our equipment is attached to, treats the call in a different fashion and routes the calls through a data link instead of through a normal voice channel. Due to the fact that "Follow Me Roaming" is activated and de-activated on a daily basis, the target instrument is assigned a temporary telephone number which changes daily. Even the target does not know what this number is. Any person involved in a criminal activity who is aware of this technology would know that, except on possibly a federal level, with the expenditure of great resources and a great amount of cooperation from the various cellular companies, this telephone cannot be intercepted. An example of how this could be used, without the target roaming around the country is as follows:

1) I travel to Washington, DC and, through a contact or my own resources, I have a cellular telephone activated, through the local carrier with a 202 area code.
2) I return to Philadelphia and activate "Follow Me Roaming."
3) Any outgoing calls made by me on this telephone would be going through the Philadelphia carrier and then into a land line. They would never even hit my home switch in Washington.
4) Any incoming calls made to my assigned 202 telephone number would automatically be forwarded to me in Philadelphia to the telephone number that my instrument had been temporarily assigned on that particular day. This process would be completely transparent to any intercept equipment attached to the switching office in my home area. It would appear, to anyone monitoring my telephone, that it was not in use.

As long as I kept my bill current with the mobile telephone company, I could do this indefinitely.

Another problem that we have encountered with the telephone company is the installation of a trap and trace on a telephone number assigned to a pager. The position of Bell of PA is that this cannot be done by them but must be done by the paging company. I disagree with the telephone company and feel that this is an instance where their legal department does not want to get involved in a potential problem with a large customer (i.e. a paging company). The paging company is only responsible for what is being sent out over the air. Until the incoming call connects with the paging company's computerized equipment, it is handled by the local telephone company just like any other call. This means that the telephone number of the pager, just like your home telephone number, appears on a frame in a switch and is routed through the telephone equipment just like any other call. Once it hits the paging company's computer, it then becomes their responsibility. In fact, in all other states that have the Caller I.D. function, the paging companies are able to pass the incoming telephone number on to the pager. This is information that they receive from the telephone company. We have been unsuccessful in getting Bell of PA to comply with any court order to date. This is an issue that should be specifically addressed by the Digital Telephony and Communications Privacy Improvement Act of 1994 and made applicable to all telephone companies (Baby Bells, or otherwise) as well as to those companies whose business interacts with local and national phone companies.

Sincerely,

LYNNE ABRAHAM,
District Attorney.

U.S. DEPARTMENT OF JUSTICE,
FEDERAL BUREAU OF INVESTIGATION,
Washington DC, January 5, 1994.

Mr. CASIMIR S. SKRZYPCZAK,
President, NYNEX Science and Technologies, Inc.,
White Plains, NY.

DEAR MR. SKRZYPCZAK: Upon receipt of your November 8, 1993, letter, my staff and I conducted a careful and detailed review of the results of the industry working group, which was formed at the request of industry, in March 1992 to address the electronic surveillance requirements of our Nation's state and federal law enforcement agencies. According to senior telecommunications executives, this group was to be "the approach" to address law enforcement's concerns in this area. Although the efforts of industry have been useful to a degree, an honest and candid assessment of the results achieved to date, unfortunately, leads me to conclude that this body does not appear to be equipped or able *to develop and implement* the solutions that are needed to remove the current and emerging impediments which prevent or hinder law enforcement agencies in executing court orders for electronic surveillance. Although I have held out hope that the industry working group, the Alliance for Telecommunications Industry Solutions (ATIS), and the Electronic Communications Service providers Committee (ECSPC) would provide a mechanism for achieving solutions and removing the impediments, this recent assessment compels me to acknowledge that these efforts have been inadequate.

As I mentioned in my letter of September 28, 1993, at the outset, back in March 1992, we were pleased with and supportive of the committee's mission to resolve this significant threat to the public safety, national security, and effective law enforcement. To aid in the initiative, we have devoted FBI technical experts and engineers to this process, as well as funding a telecommunications consulting firm to facilitate meetings, provide subject matter expertise, and prepare written contributions. Also, as I previously mentioned, some of the industry representatives have worked hard and appear to have been sincere in their efforts to reach solutions. However, some companies have not supported these efforts and others have not contributed meaningfully to the effort. In my estimation, this is a result of the voluntary basis and elective nature of the working group and committee approach. Particularly troubling is the fact that new service providers who are now entering the marketplace are unaware of law enforcement's requirements, and efforts by the FBI to have these requirements brought to the attention of industry standards bodies, such as the one now considering personal communications Services (PCS) systems, were not supported by industry representatives in the committee.

I believe that in order to successfully accommodate law enforcement's needs and to ensure that electronic surveillance responsibilities are discharged as new technologies emerge, a mechanism must exist that, in a certain and comprehensive fashion:

- Identifies fully law enforcement's electronic surveillance requirements to the telecommunications industry;
- Prompts the technical solutions necessary to meet the requirements of law enforcement;
- Assures timely implementation of these solutions into the telecommunications industry's existing and emerging technologies; and
- Addresses the cost issues associated with the technical solutions and their implementation.

Time has shown that the ECSPC, by itself, is not capable of achieving our goal of ensuring the ability of law enforcement to perform electronic surveillance without fail within existing and emerging telecommunications systems.

As I have previously indicated, the efforts of many committee members have been greatly appreciated by law enforcement. However, it is apparent that the recommended industry approach, the ECSPC, cannot address all of the necessary elements I have listed above. In fact, several committee members have made the point that, as matters stand, only an individual company can determine whether or not it is willing to pursue and implement solutions once they are identified.

It is my view that the committee process should be a mechanism for discussing law enforcement needs *and identifying technical solutions.* Committee products thus far, such as those reflected in the ISDN, Digital Loop Carriers, and Cellular action teams' written recommendations, have not included solutions, but rather have largely only restated law enforcement's current abilities and limitations in performing electronic surveillance in these technical environments—information which the FBI itself provided nearly two years ago. In the main, these products observe the need for the development of solutions to meet law enforcement needs, but they do not provide these solutions. Inasmuch as the committee is not empowered to resolve cost and other issues key to the implementation of solutions, the lack of meaningful and timely solutions to these technological problems will continue.

As we have indicated previously, we shall continue our active participation in the committee process. However, given the results to date, we are also obligated to pursue other approaches which will ensure law enforcement's continued ability to protect the safety and economic well-being of the American public through the use of this essential investigative technique.

Sincerely yours,

JAMES K. KALLSTROM,
Special Agent in Charge.

TELECOMMUNICATIONS INDUSTRY SOLUTIONS,
Washington, DC, March 1, 1994.

Mr. JAMES K. KALLSTROM,
Special Operations Division,
Federal Bureau of Investigation, New York, NY.

DEAR JIM: I am writing in response to your letter of January 5, 1994, in which you expressed your concerns regarding industry efforts to address the electronic surveillance requirements of state and federal. law enforcement agencies.

First, let me say that your observations regarding the functioning of the Electronic Communications Service Provider Committee (ECSP) and its progress to date in resolving issues are understandable. These comments included: the Committee is not equipped to implement the technical solutions which it identifies; some companies have not supported these efforts and others have not contributed meaningfully to the effort; and efforts by the FBI to have law enforcement's requirements brought to the attention of industry standards bodies were not supported by all representatives on the Committee. However, these observations which you find troubling are aspects of the committee process which are fundamental to the operation and interest of open industry forums.

One of the basic principles of any inter-industry committee or forum is that solutions reached are proposals for voluntary implementation by the participants: recommendations are non-binding. While each participant is committed to good faith discussions and consideration of timely implementation, each company represented also reserves fully independent judgment in terms of any implementation. This tenet of operation serves a number of purposes, a key one being that it litigates the legal/antitrust risks of conducting these discussions in any industry meeting.

The forum process also ensures that there is careful consideration of all views and objections, appropriate notification and opportunity for the industry to review and provide comments on any proposed solution, and ultimate resolution by consensus. While there is no guarantee, the fact that all participants have been a part of these sensitive discussions, have been afforded due process, and have willingly expended the necessary resources in the development of a solution more often than not results in strong incentives to implement. It simply may not produce the direct and open commitment to implement solutions at the Committee level that you appear to be looking for.

As I am sure you are aware, most of the solutions developed or being discussed are costly to implement, and can require months, even years to develop. Quite frankly, decisions of this magnitude require review by higher levels of management than those representatives present at the ECSP Committee. Industry sends the subject matter experts to these meetings to develop the technical solutions. Typically, industry does not send representatives who are authorized to make business decisions which may involve large expenditures. While you may view that as a shortcoming of this industry process. I believe that federal agencies operate in the same fashion.

Another characteristic of industry forums is that participating companies do not support and/or contribute to efforts equally. Participants tend to gravitate toward and contribute to those issues in which they have the most interest or the greatest business need. They rely on other participants to provide leadership on the remaining issues. Over time, leadership and contributions tend to balance. Evaluating an individual company's commitment to the process by its level of participation on a single issue can possibly provide a distorted view. The fact that a particular company is not among the leaders on a particular issue does not mean it is not aware or does not care about what is being discussed. The minutes or notes of all meetings, as well as the contributions discussed, are available to all participants for review and comment; and I assure you they are scrupulously reviewed. The stakes are simply too high for them to be ignored. Even though resolutions and recommendations are non-binding, no company wishes to be part of a consensus it cannot ultimately support.

Your concern that efforts by the FBI to have law enforcement's requirements brought to the attention of industry standards bodies were not supported by all industry representatives on the Committee, has proved short lived. At the October meeting the Committee agreed to provide a contribution to the Joint Experts Meeting (JEM) on Privacy and Authentication for Personal Communications held November 8–12. It was reported at the December 1993 Committee meeting that at the GEM the law enforcement requirements were presented and discussed. The Committee observed that the "objective to raise awareness of the needs of law enforcement to support surveillance were met." At the most recent meeting of the ECSP Committee. The PCS action team was empowered by the full committee to prepare and submit contributions to a number of standards bodies addressing PCS issues. The initial reluctance of the Committee to support this effort was no doubt due to the short turn-arounds required to prepare and approve contributions, and the fact that both industry and law enforcement continue to insist that nearly all Committee documents be considered proprietary. The standards process is an open, public process which requires that all contributions submitted be nonproprietary. Similarly, if new service providers are to become aware of law enforcement's requirements, those requirements must be publicly available. To date, the Committee has been reluctant to publicize these requirements in the belief that to do so will serve to highlight current shortcomings.

Even though discussions between law enforcement and industry have been ongoing for some time, this particular committee, which is co-chaired by industry and law enforcement, and its incumbent operating principles, has been in existence for less than one year. participants are only now gaining the mutual respect required to bring forth meaningful solutions. You noted the fact that the Committee's products to date merely "observe the need for the development of solutions to meet law enforcement needs." I see this as a necessary step forward. If meaningful solutions are to result, all participants must first understand that there is in fact a problem, not that one participant, or one group of participants, says so. Now that the Committee recognizes the problems, it can proceed to identify and develop appropriate solutions.

I understand your obligation to pursue whatever approaches you deem necessary to ensure law enforcement's continued ability to conduct the lawful intercept of communications. However, whatever those other approaches may be, and whatever results those approaches may yield, it will still be necessary for industry and law enforcement to work together to identify and develop suitable technical solutions. I believe the ECSP Committee is the appropriate forum for that purpose.

Sincerely,

CASIMIR S. SKRZYPCZAK,
ATIS Chairman.

GAO

United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

B-249358

July 17, 1992

The Honorable Edward J. Markey
Chairman, Subcommittee on
Telecommunications and Finance
Committee on Energy and Commerce
House of Representatives

Dear Mr. Chairman:

In March 1992, you asked us to evaluate the (1) technological alternatives available or imminently available to the Federal Bureau of Investigation (FBI) to wiretap voice and data communications,[1] (2) changes required to the telecommunications network to accommodate least intrusive wiretaps,[2] and (3) estimated cost of developing and implementing such changes. On June 26, 1992, we briefed your office on the results of our evaluation. At that time, we also discussed the FBI's past and current actions to satisfy its wiretapping needs, including its April 1992 proposal to amend the Communications Act of 1934 and its May 1992 proposal for separate legislation to provide for its wiretapping needs by the telecommunications industry. This report documents our briefing. Appendix I contains the slides we used at that briefing.

The FBI has classified our analysis of the technological alternatives to wiretapping as National Security Information. In this regard, we provided your office with a classified briefing on our analysis on June 15, 1992.

Results in Brief

The technological wiretap alternatives available to the FBI and the network changes needed to accommodate the least intrusive wiretaps vary depending on the technology used. However, neither the FBI nor the telecommunications industry has systematically identified the alternatives, or evaluated their costs, benefits, or feasibility

The FBI, in its April 1992 legislative proposal, did not define its wiretapping needs. The May 1992 proposal generally addressed the FBI's needs, but did not provide specifics necessary for the telecommunications industry to determine what would constitute full compliance with the proposal in the event it were enacted. For example, the proposal did not specify the length of time allowed to install a wiretap after receipt of a court order. Further, the May 1992 proposal did not address who should pay for the cost of wiretapping solutions. FBI and industry officials have recently begun working together to identify technological alternatives available to the FBI for wiretapping and to select the alternatives that best meet their needs.

---

[1] Wiretapping refers to the real-time collection of dialed digits and sending of real-time, two-way communications to a listening device, regardless of the target's location or the technology used. Real time means collecting and sending this information to a listening device as it is being communicated.

[2] The term intrusive refers, for purposes of this report, to the level of the wiretap's detectability by the wiretap's target.

Background

The FBI considers wiretapping an essential information gathering tool in fighting crime. The federal government and 37 states have statutes governing wiretapping.

The FBI now has the technical ability required to wiretap certain technologies, such as analog voice communications carried over public networks' copper wire. However, since 1986, the FBI has become increasingly aware of the potential loss of wiretapping capability due to the rapid deployment of new technologies, such as cellular and integrated voice and data services, and the emergence of new technologies such as Personal Communication Services, satellites, and Personal Communication Numbers.

In response to the rapidly changing technology, the FBI prepared two legislative proposals in April and May 1992. The May proposal replaced the April proposal.[3] According to the FBI, these proposals are intended to maintain the same level of wiretapping capability for new telecommunications technology that it has with technologies such as older analog communications using copper wire.

Technological Alternatives and Network Changes Required to Implement Least Intrusive Wiretaps Vary With the Technology

There are six current or imminent telecommunications technologies that the FBI needs to be able to wiretap. These are (1) analog and digital using copper wire transport, (2) analog and digital using fiber optic transport, (3) Integrated Services Digital Network (ISDN), (4) Private Branch Exchange (PBX), (5) broadband, and (6) cellular. There are also three future technologies for which wiretapping capabilities need to be addressed: (1) satellite switches, (2) Personal Communication Services (PCS), and (3) Personal Communication Number (PCN). Further, the FBI needs to be able to wiretap any special features such as call forwarding or electronic mail.

---

[3] The May proposal has not been formally introduced as legislation in either the Senate or the House of Representatives

Wiretapping can occur at six primary locations through which the communications flow—at the premises where the target is located, between the premises and the cross-connect,[4] at the cross-connect, or at a land line, cellular, or satellite switch.

The technological alternatives for wiretapping vary with the telecommunications technology being tapped and the location where the tap occurs. For example, the technology used to tap a nondigital telephone is different from that used to tap a digital telephone. Further, tapping at the premises may require a different technology from tapping at a switch. Similarly, the network changes needed to implement the least intrusive wiretaps vary by technology and location.

Because the FBI has classified our analysis of these alternatives as National Security Information, we are not presenting them in this report.

No Comprehensive Studies Exist Identifying Alternatives and Their Costs, Benefits, and Feasibility

As of June 30, 1992, neither the FBI nor the telecommunications industry had systematically identified the alternative approaches for implementing minimally intrusive wiretapping capabilities and the costs, benefits, and feasibility of these alternatives.

The FBI's and telecommunication industry's past efforts to identify technological alternatives have been unsuccessful. In the past, the FBI met with security officers within the telephone companies to effect wiretaps. According to the FBI and industry officials, these security officers were the designated company contacts for meeting the FBI's wiretapping needs.

However, industry security officers did not discuss the FBI's wiretapping needs with the industry's technical experts who develop the technologies. Consequently, these experts were not informed of the FBI's needs and were not involved in identifying technological alternatives and solutions until July 1990, when the FBI began technical discussions with them.

In addition, while the FBI conducted its own research on wiretapping, these research efforts were not coordinated with industry research and development. As a result, neither the FBI nor the telecommunications industry had a comprehensive analysis of the technological alternatives for wiretapping current and emerging technologies.

---

[4] The cross-connect is located at the central office of the telephone company; this is where transmissions are converted from one form to another, e.g., from analog to digital.

Recent FBI Actions to Define and Communicate Its Wiretapping Needs

Recently the FBI has taken actions to better define and communicate its wiretapping needs to the telecommunications industry.

The April 1992 proposal to amend the Communications Act of 1934 did not define the FBI's wiretapping needs. In contrast, the May 1992 proposal for separate legislation, which replaced the April proposal, contains specific high-level discussion of its needs. For example, the May proposal states that tapped data must be in the same form as that received by the target and the data must be in real time, independent of the target's location, undetectable, and capable of being transmitted to a listening device. It also specifies time limits for meeting the FBI's needs and gives the Department of Justice the authority to ensure compliance or grant exemptions.

However, the May proposal does not address what the telecommunications industry would need to do to be in full compliance with the proposal in the event it is enacted, the meaning of certain technical terms, or who would pay for the cost of wiretapping solutions. For example, the proposal did not specify the length of time allowed to install a wiretap after receipt of a court order. According to the FBI, it will address compliance in its wiretapping requirements document, which is being developed. The proposal also does not address the international implications of future technologies, such as PCN, on wiretapping. PCN will involve assigning a subscriber one telephone number. All calls will be billed to that number regardless of what instrument or network the subscriber uses. Using PCN, the subscriber may be anywhere in the world, and the service may be provided by any service provider using any technology. Since some of the service providers may be international, and since the providers may be outside the United States, the FBI will have to establish cooperative arrangements with foreign law enforcement agencies in order to wiretap.

In May 1992, the FBI formed a technical committee composed of staff from the FBI and the telecommunications industry. The purpose of this committee is to identify technological alternatives and select the alternatives that best meet the FBI's needs. As of June 1992, the committee was developing its charter. These FBI efforts are steps in the right direction.

Scope and Methodology

We identified and assessed the technological alternatives for wiretapping in the following technologies: (1) analog and digital using copper wire transport, (2) analog and digital using fiber optic transport, (3) ISDN, (4) PBX, (5) broadband, (6) cellular, (7) satellite, (8) PCS, and (9) PCN. As part of our assessment, we also analyzed the wiretapping implications of special features associated with these technologies, such as call forwarding and voice mail. On the basis of our analysis of the technologies and discussions with representatives of the telecommunications industry, we identified the six primary wiretapping locations.

We also assessed the FBI's past and current actions to satisfy its wiretapping needs, including its April 1992 proposal to amend the Communications Act of 1934, and its May 1992 proposal.

We met with the FBI's Assistant Director and Deputy Assistant Director (Operations), Technical Services Division, and technical managers from the FBI Engineering Research Facility to discuss the FBI's progress in defining and communicating its wiretapping needs. We also held technical discussions on the above technologies with four Bell operating telephone companies, two switch manufacturers, two cellular providers, two cellular and satellite manufacturers, and the associations of the International Chiefs of Police and Major Cities Chiefs of Police. In addition, we contacted the National Security Agency, which told us that it does not have expertise in these areas. We performed our work at FBI's headquarters office in Washington, D.C., and Engineering Research Facility in Quantico, Virginia, as well as at the corporate offices of the industry representatives visited in various locations nationwide.

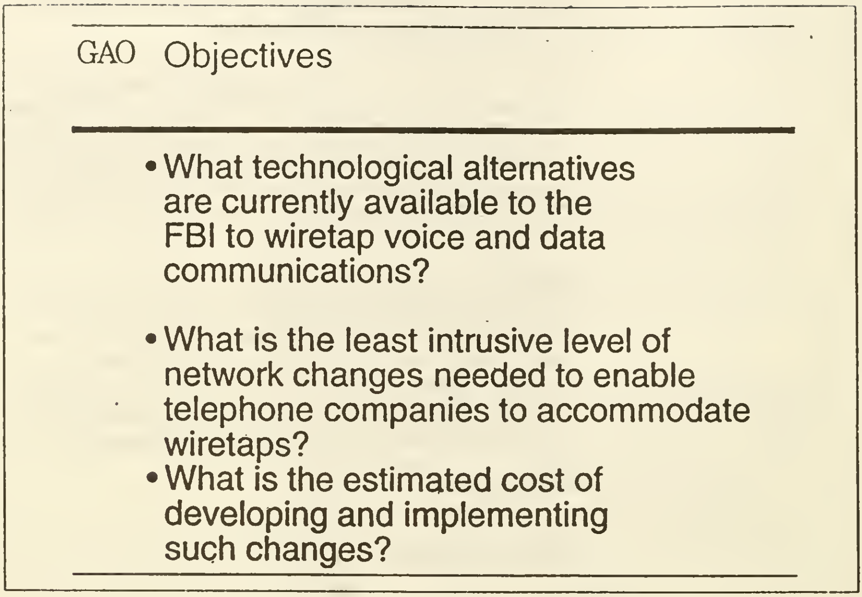
Our work was performed between April and June 1992 in accordance with generally accepted government auditing standards.

We did not obtain written comments on this report. However, we briefed FBI officials, including the Assistant Director and Deputy Assistant Director (Operations), Technical Services Division, on the results of our work and on our discussions with the telecommunications industry. These officials generally agreed with the facts as presented, including our technical assessment of the wiretapping alternatives. We have incorporated their views, as well as their updates on the FBI's planned actions, in the report as appropriate.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan to make no further distribution until 30 days from the date of this letter. We will then send copies to the Attorney General; the Director of the Federal Bureau of Investigation; the Director, Office of Management and Budget; and interested congressional committees. Copies will also be made available to others upon request. This report was prepared under the direction of Howard G. Rhile, Director, General Government Information Systems, who can be reached at (202) 512-6418. Major contributors to this report are listed in appendix II.

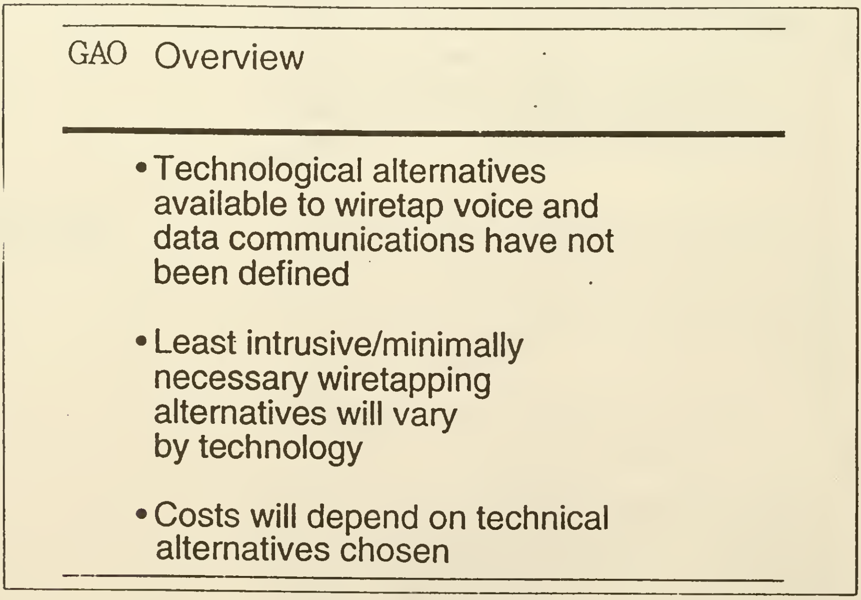
Sincerely yours,

For Ralph V. Carlone
Assistant Comptroller General



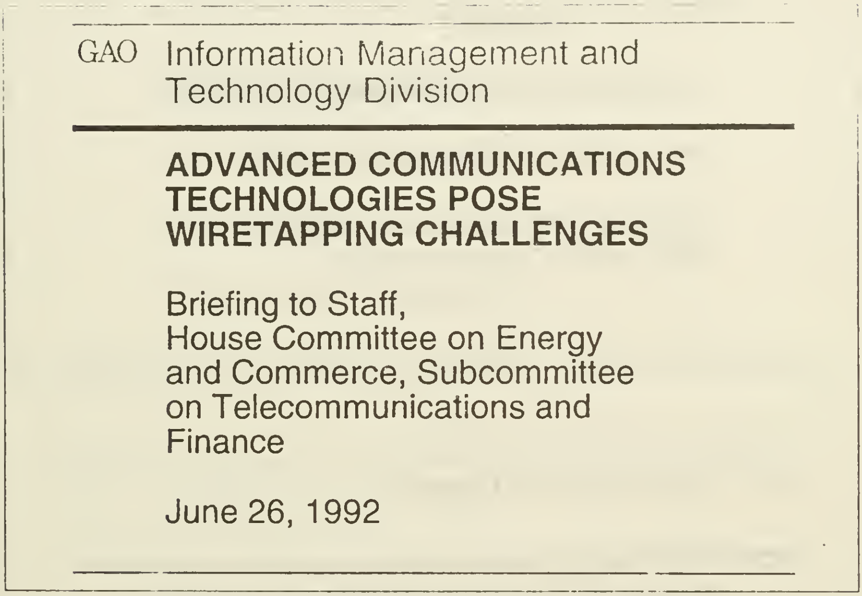
GAO Objectives

- What technological alternatives are currently available to the FBI to wiretap voice and data communications?
- What is the least intrusive level of network changes needed to enable telephone companies to accommodate wiretaps?
- What is the estimated cost of developing and implementing such changes?



GAO Overview

- Technological alternatives available to wiretap voice and data communications have not been defined
- Least intrusive/minimally necessary wiretapping alternatives will vary by technology
- Costs will depend on technical alternatives chosen

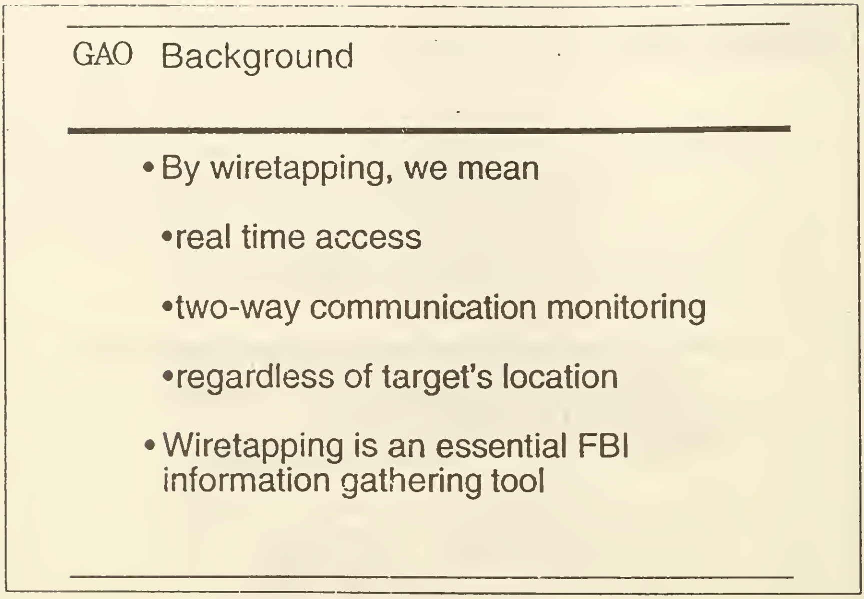


GAO Information Management and Technology Division

ADVANCED COMMUNICATIONS TECHNOLOGIES POSE WIRETAPPING CHALLENGES

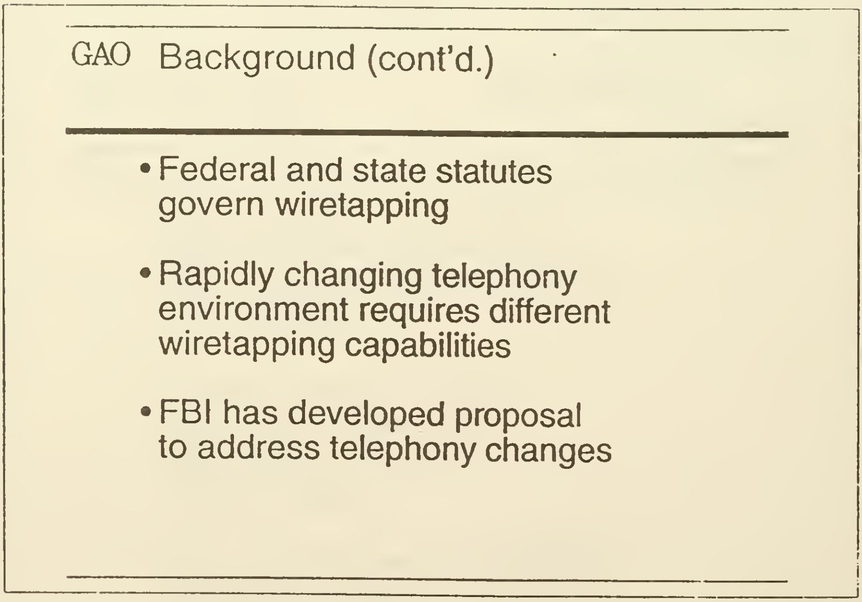
Briefing to Staff,
House Committee on Energy
and Commerce, Subcommittee
on Telecommunications and
Finance

June 26, 1992



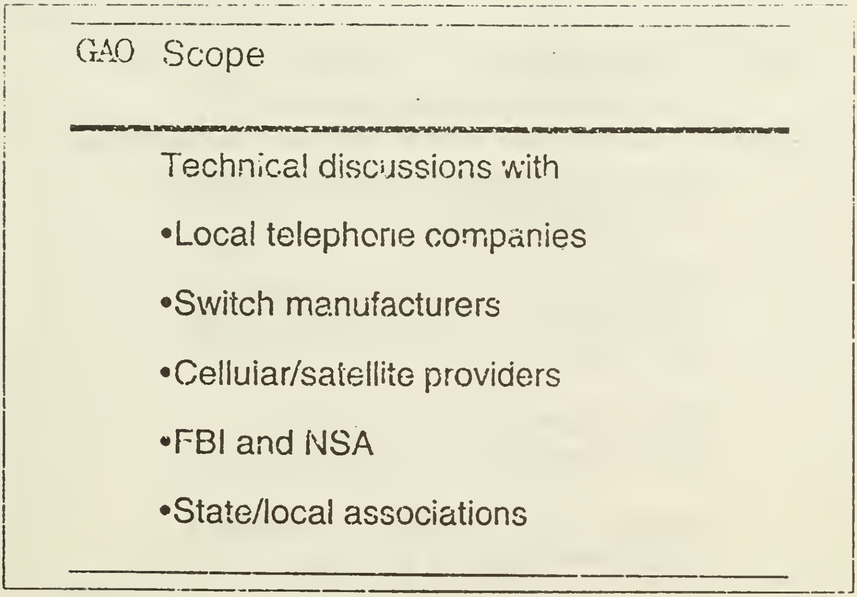
GAO Background

- By wiretapping, we mean
  - real time access
  - two-way communication monitoring
  - regardless of target's location
- Wiretapping is an essential FBI information gathering tool



GAO Background (cont'd.)

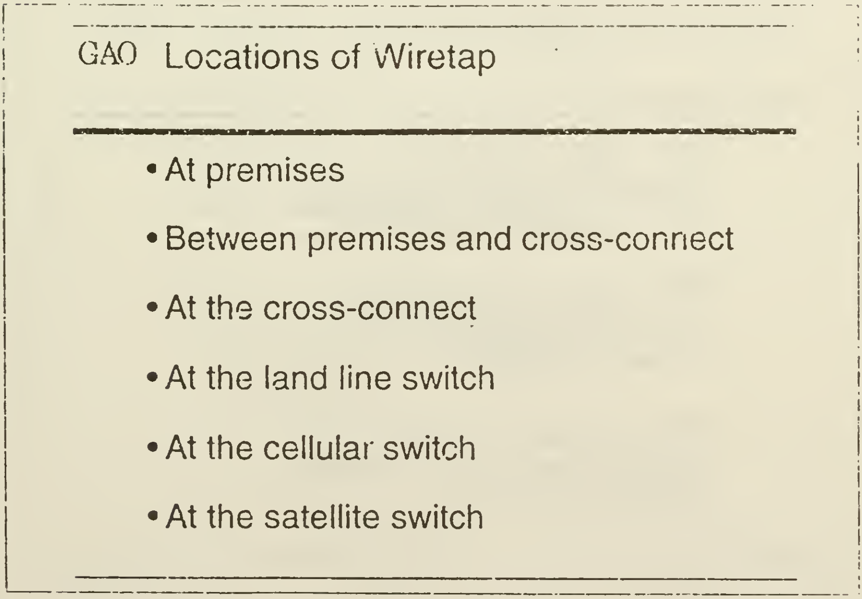
- Federal and state statutes govern wiretapping
- Rapidly changing telephony environment requires different wiretapping capabilities
- FBI has developed proposal to address telephony changes



GAO Scope

Technical discussions with

- Local telephone companies
- Switch manufacturers
- Cellular/satellite providers
- FBI and NSA
- State/local associations



GAO Locations of Wiretap

- At premises
- Between premises and cross-connect
- At the cross-connect
- At the land line switch
- At the cellular switch
- At the satellite switch

GAO Past Attempts to Define Alternatives Unsuccessful

- Law enforcement wiretapping needs not clearly defined
- FBI/industry technical discussions on wiretapping needs not begun until July 1990
- FBI research not coordinated with industry
- Unclear responsibility for cost and implementation of technical solutions

GAO FBI Corrective Actions

- May 1992 - Drafted wiretapping requirements and proposed legislation
- May 1992 - Established technical committee with industry officials
- Continuing to conduct independent research to find technical solutions

GAO May 1992 Proposal to Clarify Wiretapping Responsibilities

- Provides general FBI wiretapping needs to maintain current wiretapping capabilities
- Specifies industry responsibilities and time limits for meeting FBI's needs
- Gives Justice authority to ensure compliance or grant exceptions

GAO What Is Not Addressed in Proposal

- Specifics on what is full compliance (e.g., response time, sizing, etc.) and the meaning of technical terms
  - Draft May 1992 wiretapping requirements intended to provide specifics on full compliance
- Who pays for the cost of solutions

GAO Costs

- Cost and feasibility studies on the changes needed have not been conducted
- Least intrusive/minimally required tapping method may increase costs
- Industry may seek reimbursement through government agencies

GAO Overall Assessment

- FBI is finally moving in right direction to define its wiretapping needs and communicate with industry
- FBI still needs to
  - Finalize wiretapping needs including specifics on what is meant by full compliance and by technical terms
  - Resolve cost and feasibility of technical alternatives and solutions
  - Define least intrusive/minimally necessary alternatives for each technology
  - Also, FBI needs to work with foreign law enforcement agencies to establish cooperative agreements for wiretapping foreign service providers of new, emerging technology

Appendix II

Major Contributors to This Report

Information Management and Technology Division, Washington, D.C.	William D. Hadesty, Technical Assistant Director Dr. Rona B. Stillman, Chief Scientist Stephen A. Schwartz, Assistant Director Brian C. Spencer, Evaluator-In-Charge Robert C. Sorgen, Senior Evaluator
Office of General Counsel	Raymond J. Wyrsch, Legal Counsel

ORGANIZED CRIME APPENDIX

The President's Commission on Organized Crime stated the following conclusions in its report, *The Edge: Organized Crime, Business and Labor Unions:*

- If unchecked, organized crime can take over, own, and operate legitimate business. It can also control entire industries. The ways in which industry can be affected are by the increased price of items due to theft, bribery (kick-backs), price fixing and the control of trade.
- The control of the marketplace by organized crime is also obtained by tile control of unions and by monopolizing power in specific industries.
- Through the control of unions, payoffs can be demanded to ensure labor peace. Businesses comply with the labor union's demands rather than lose profits or lose business. Another deleterious effect of organized crime control is through the illegal utilization of union funds. At the time of the report of the PCOC, union benefit funds had cumulative assets of over $51 billion. Influence in the unions on a local level, if strong enough, may lead to control of the union at the international level.
- The costs of labor racketeering are hard to trace. The Commission estimated that millions of dollars in workers' labor union dues were stolen from the unions through embezzlement, lost through illegal loans, and taken through extortionate and illegal fees paid to trust and service fund providers.

As a result, the U.S. public is forced to pay higher commodity costs because of organized crime's control. Examples cited by the Commission of the various types of economic loss are:

- Amalgamated Local 355, an independent union in Queens, New York, lost nearly $2 million in a kickback and embezzlement scheme in the mid-1970's. The scheme involved the union's secretary/treasurer and a well-known real estate developer.
- The control of the concrete industry by the LCN in New York, as brought out in the LCN Commission indictment, was demonstrated in evidence which showed that over the period 1981–1984, the 2 percent skim collected on the total cost of poured concrete, on the delivery of it to the job site, and on the attendant labor costs could range anywhere from $1.6 to $3.5 million. This figure was estimated on the control of the concrete industry alone. Increased construction costs then lead to higher overall building project costs and increased rental rates, etc. Essential evidence supporting this prosecution was derived from electronic surveillance.

Through the utilization of electronic surveillance, Federal and state investigations continue to have a significant impact upon organized crime groups. In Fiscal Year 1991, at the Federal level, there were 239 recorded convictions and 246 indictments of LCN members and associates. In addition, civil RICO complaints spawned by the criminal investigations were filed against 25 individuals and/or entities, and judgments were entered against 23. Aggressive use of the seizure and forfeiture provisions of the RICO statute yielded $17,554,865. Over $11,779,106 in fines were levied against convicted individuals; recoveries and restitutions totaling $22,881,539 were obtained; and $7,044,625 in potential economic losses were prevented. A few recent cases, wherein electronic surveillance played a critical role, illustrate the importance of maintaining the efficiency of this investigative technique.

- *Commercial seafood and longshoremen dock-loading industries.* For over 70 years, organized crime, and particularly the Genovese LCN family, had dominated and controlled the Fulton Fish Market and its immediate environment in New York City. Through electronic surveillance which spanned over two years, the government acquired substantial evidence as to the influence and control of organized crime in the seafood industry and the labor unions related to it. As a result, in October 1987, a civil RICO complaint was filed against the Genovese LCN crime family, certain unions controlled by organized crime, and a number of LCN members and associates. In 1988, in a landmark RICO decree and judgment, the Fulton Fish Market was placed under the oversight of a court-appointed administrator. Judgments in this civil RICO action permanently bar the Genoves LCN crime family and other defendants from having any future dealings in that seafood market.

Although it is difficult to quantify the impact of the government's intervention into this industry, the enormous economic and social costs associated with the LCN's control of this market have been significantly reduced. Illegal activities such as hijacking, gambling, robbery, burglary, loansharking, extortion, murder, narcotics trafficking, and labor racketeering flourished in the Market's environment while under the dominion of the LCN. These activities have dramatically abated with the imposition of the consent and default judgments. The court-appointed administrator and other independent sources of information, such as the media, report that the Fulton Fish Market has sales approximating two billion dollars annually. Seafood that passes through the market is bought and sold throughout the United States. Illegal activity at the Market has inflated seafood costs by $1–2 dollars per pound and virtually every household in America has absorbed that cost. By a conservative estimate, the American public has been spared literally millions of dollars in increased seafood costs as a result of this investigation.

- *International Longshoremen's Association.* This investigation focused primarily upon corruption on the New York and New Jersey waterfront the second largest port in the world. The civil RICO. complaint names as defendants the International Longshoremen's Association (ILA), their executive boards, six local labor unions, and 32 present or former officials of these ILA locals, 21 of whom are identified as members or associates of the Gambino and Genovese LCN crime families, and the "Westies" criminal gang. Twelve additional individuals are identified in the complaint as members or associates of the Gambino and Genovese LCN families and the Westies, and several employers in industries affecting waterfront commerce are named for purposes of obtaining adequate relief.

The complaint alleges that the LCN figures have used these locals and their various affiliated benefit funds to conduct a pattern of racketeering activity on the waterfront, which includes murder, extortion, embezzlement of union funds, illegal labor and benefit fund payments and mail fraud. To prove such wide-ranging conspiracies, the type of evidence needed typically requires substantial reliance upon electronic surveillance-based information.

These investigations, which heavily relied upon electronic surveillance, demonstrated an extraordinary breadth of control by the Genovese LCN family over waterfront activity that extended from the New York—New Jersey piers all the way to the Port of Miami. This pervasive control by organized crime over the waterfront extends back to the turn of the century. Organized crime obtained this control by its early recognition that to transport goods to the eastern seaboard, markets often required passage through the New York/New Jersey waterfront, and that this transportation terminal point presented a labor intensive bottleneck. To control waterfront labor, thus, was to exercise tremendous leverage over the entire shipping industry, effect the commerce of a huge section of the American economy, and ultimately to drive up prices of a myriad of commodities sold in the United States.

There are numerous other examples where, through the use of court-ordered electronic surveillance, major economic harm was abated. The nationwide investigation into organized crime-labor racketeering influence in the union health and dental care industry has resulted in the termination of frauds and kickbacks which cost unions and insurance companies millions of dollars. In one investigation, sixteen different FBI field offices were involved, eight of which conducted extensive electronic surveillance. At the conclusion of the investigation in September, 1988, seven separate Federal Grand Jury indictments were returned in Atlanta, Chicago, Baltimore, San Diego, and San Francisco, charging ten individuals and five corporations with numerous Federal violations including RICO, conspiracy, mail fraud, wire fraud, and labor racketeering. As a result of this investigation, ten health care executives were convicted, the U.S. Public Health Service changed its bidding procedures nationwide, SAFECO Insurance Company terminated its practice of paying double commissions to insurance agents nationwide, and spin-off investigations resulted in the conviction of a Federal judge and two labor-related, organized crime leaders.

Electronic surveillance was extensively utilized in the landmark civil RICO investigation called "Liberatus" which resulted in the formal break up of LCN control over the nation's largest union, the International Brotherhood of Teamsters. The LCN's grip over this union had been intact since the 1950's. As a result, for the first time in decades the nation's largest union is free from organized crime control and corruption, and the continued pillage of union funds has ceased.

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL ADOPTED SUMMER MEETING JULY 8–11, 1992, PITTSBURGH, PENNSYLVANIA

RESOLUTION SUPPORTING LEGISLATION TO CLARIFY THE RESPONSIBILITY OF TELECOMMUNICATIONS COMPANIES TO ASSIST LAW ENFORCEMENT WITH COURT-AUTHORIZED ELECTRONIC SURVEILLANCE IN LIGHT OF NEW TECHNOLOGIES

WHEREAS, one of the most important and effective tools used by federal, state and local law enforcement in the investigation of criminal activities is the court-authorized interception of communications or wiretapping; and

WHEREAS, 37 states and the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation authorizing their state and local law enforcement agencies to conduct court-authorized electronic surveillance in criminal investigations; and

WHEREAS, approximately 60 percent of the court-authorized wiretaps conducted annually in the United States are by state and local law enforcement agencies; and

WHEREAS, federal and state electronic surveillance statutes set forth a procedure for obtaining judicial authorization to conduct electronic surveillance and require the telecommunications industry and others to provide law enforcement with "all information, facilities, and technical assistance necessary to accomplish the interception," 18 U.S.C. §§2518(4) and 3124(a)(b); and

WHEREAS, the telecommunications industry is introducing, and has introduced, a number of advanced technologies, including digital technology which facilitates the simultaneous transmission of multiple commingled communications, impeding the ability of law enforcement to lawfully intercept specific communications to the exclusion of all other communications not the target of electronic surveillance; and

WHEREAS, modifications to certain of these advanced technologies are required so that law enforcement can continue its use of court-authorized electronic surveillance to intercept the communications of persons engaged in criminal conduct, to the exclusion of others; and

WHEREAS, legislation has been proposed that requires telecommunications and other electronic communication service providers, when authorized by law, to provide law enforcement with the capability of intercepting the entire content of communications of persons engaged in criminal conduct, to the exclusion of all others, regardless of the technology involved;

Now, therefore, be it resolved that the National Association of Attorneys General:

1) Supports legislation which requires telecommunications and other electronic communication service providers, when authorized by law, to provide law enforcement with the capability of intercepting the entire content of communications of persons engaged in criminal conduct, to the exclusion of all others, regardless of the technology involved; and;
2) encourages Congress to adopt such legislation; and
3) authorizes the Executive Director and General Counsel to transmit these views to the Administration, the Congress and other interested organizations and individuals.

Abstains: Attorney General Chris Gorman

NATIONAL DISTRICT ATTORNEYS ASSOCIATION

RESOLUTION CONCERNING THE DIGITAL TELEPHONY AND COMMUNICATIONS PRIVACY IMPROVEMENT ACT

WHEREAS, one of the most important and effective technique's used by state, local and federal law enforcement in the investigation of complex and life threatening criminal activities is the court-authorized interception of otherwise private communications (wiretapping), and

WHEREAS, 37 states and the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation authorizing their state and local law enforcement agencies to conduct court-authorized electronic surveillance and establishing administrative and judicial oversight procedures to ensure the protection of privacy interests; and

WHEREAS, approximately 56 percent of the court-authorized wiretaps conducted annually in the United States are by state and local law enforcement agencies; and

WHEREAS, both federal and state electronic surveillance statutes set forth a procedure for obtaining judicial authorization to conduct a wiretap and require the telecommunications industry and others to provide "all information, facilities, and technical assistance necessary to accomplish that interception," 18 U.S.C. Sec. 2518(4) and 3124(a)(b); and

WHEREAS, the rapid and continual development of new telecommunications technologies and services present an ever increasing barrier to accomplishing the court-authorized electronic surveillance; and

WHEREAS, modifications to these new technologies and services are required to effectuate the intent of federal and state statutes to permit court-authorized electronic surveillance of the communications of persons engaged in serious and life threatening criminal conduct and protect the privacy of others; and

WHEREAS, the Digital Telephony and Communications Privacy Improvement Act (the "Act") requires the telecommunications industry, when authorized by law, to provide law enforcement with the capability of intercepting the entire content of communications of persons engaged in criminal activities, regardless of the technology involved; and

WHEREAS, the Act requires the Federal Bureau of Investigation to provide fiscal support for the telecommunications industry to achieve this capability; and

WHEREAS, the Act enhances privacy protection for individuals using emerging technologies,

THEREFORE BE IT RESOLVED, THAT, the National District Attorneys Associations supports the Digital Telephony and Communications Privacy Improvement Act; and

BE IT FURTHER RESOLVED, THAT, this Association urge the Congress to enact the Digital Telephony and Communications Privacy Improvement Act.

Adopted by the Board of Directors July 24, 1994 (Newport Beach, California)

ANALYSIS OF INFORMAL SURVEY OF TECHNICAL PROBLEMS ENCOUNTERED BY LAW ENFORCEMENT IN CONDUCTING ELECTRONIC SURVEILLANCE

Last year, the Federal Bureau of Investigation, through an informal survey of Federal, state, and local law enforcement agencies, collected information regarding recent electronic surveillance court orders[1] that have been frustrated or delayed due to technology-based problems. Although this survey was conducted informally, the results provide valuable, and representative anecdotal information regarding the difficulties presently being encountered by law enforcement agencies. It would be a mistake to analyze this problem by simply counting the specific number of court orders frustrated or delayed in the past. However, by collecting and reviewing information regarding the recent problems, law enforcement agencies have come to understand the serious implications of the impacts of new and advanced technologies on their ability to conduct wiretaps, when law enforcement electronic surveillance requirements are omitted.

The survey revealed ninety-one (91) instances in which law enforcement agencies were prevented from fully implementing court orders for electronic surveillance due to various technological impediments. In reviewing the results of this survey, the following should be noted:

- The survey was intended to collect information regarding *recently encountered* problems only.
- The results do not include technological problems that are outside of the coverage of the legislation, as drafted (e.g., intercepts of Private Branch Exchange equipment).
- The results do not include impediments created by cellular carriers offering "roaming" service.
- The results do not include situations where court orders were *not sought* due to impediments known in the past to preclude effective execution of the court order. (for example, court orders not sought due to known cellular system port capacity limitations)
- The reference to encryption problems is a reference to *carrier provided* encryption, and *not user-employed* encryption devices.

Of the 91 instances of technological problems identified by law enforcement agencies, problems in cellular systems accounted for 40 with the inability to fully intercept cellular communications accounting for 24 instances. These problems ranged from a total inability on the part of the cellular provider to assist, to cellular systems that were not capable of isolating and collecting all of thee subject's telephone communications. For example, a Federal investigation of a major narcotics organization in the northeastern United States was hampered when the cellular carrier was unable to fulfill requests for court-ordered wiretaps due to the carrier's technical limitations. Also, an organized crime and drug trafficking task force investigation in the southeastern U.S. was unable to conduct a court-ordered wiretap because the carrier was unable to provide law enforcement with intercept access to the subject's long distance communications made through the cellular carrier's service. Difficulties caused by the "port capacities" of cellular systems accounted for another 10 problem instances. A cellular carrier in the south, for example, was unable to comply with a Federal court-order for dialed number information concerning a Federal public corruption investigation due to port capacity limitations. The remaining five problems with cellular systems involved the inability of cellular carriers to provide trap/trace information identifying the originator of a call transmitted through their systems. Calling features accounted for 29 problem instances, or approximately 32 percent. Of the features that created problems for law enforcement agencies, call forwarding and speed dialing were most prevalent. As an example, a regional telephone company in the mid-western U.S. was unable to provide a Federal law enforcement agency with either the content of the communications or the dialed number information concerning a subject drug trafficker's telephone as a result of the subjects use of custom calling features. Additionally, Custom Local Area Signaling Services (CLASS) such as "call back", and "caller I.D." also created problems.

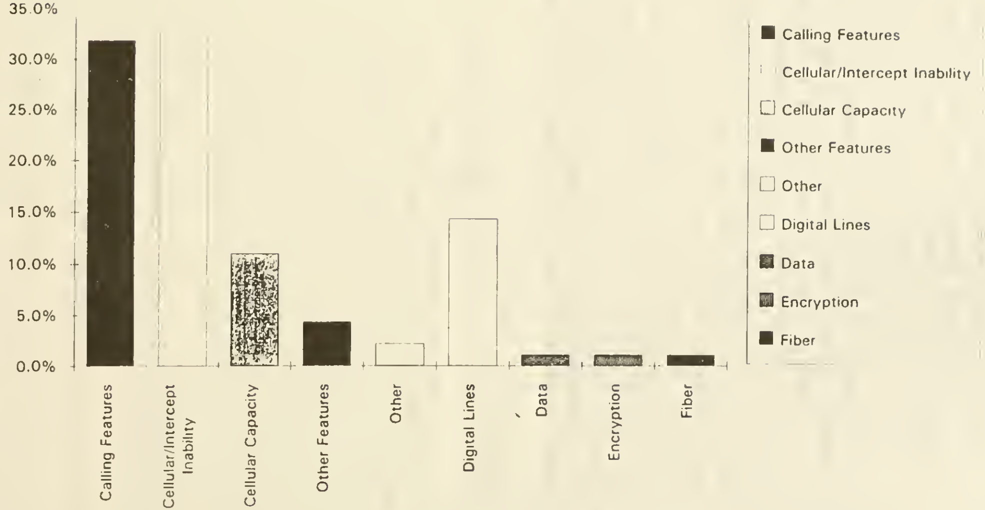
---

[1] As used here, electronic surveillance court orders refer to all court orders for criminal and foreign surveillance interceptions which capture the communication content, as well as, to the acquisition of dialed number information through pen register or trap and trace devices.

Other problems reported by Federal, state, and local law enforcement agencies included difficulties with intercepting subjects' communications due to the use of digital voice lines (13), high speed data lines (1), fiber optic cables (1) and carrier provided encryption (1).

The attached chart provides a breakdown of the reported problems encountered by the various agencies.

Technical Problems Encountered in Electronic Surveillance



PREPARED STATEMENT OF MORTON BROMFIELD ON BEHALF OF THE AMERICAN PRIVACY FOUNDATION

THE CLIPPER CHIP AND BEDROCK TELECOMMUNICATIONS PRIVACY

As part of the Clipper Chip debate, Vice President Al Gore has wisely opened the door to studying alternatives. He would balance the avowed needs of law enforcement agencies with the needs of hi-tech industry to protect this Age's "gold"—the fruits of R&D, proprietary information that CEO's pray will keep their companies six months ahead of their competition—and secure from the probing surveillance of industrial spies. And beyond this, our Vice President would see realized a national information superhighway, an "advanced nationwide network that can link classrooms, electronic libraries, rural doctors and ordinary people in their own homes." A tall order.

Mitchell Kapor, the respected founder of Lotus Development concurs, pressing for broad public access to an information highway. But several months ago Mr. Kapor, in a NY Times article [Nov. 24, 1993, p. A15] cautioned, "People won't use the new technology unless they feel that their privacy is protected."

Strictly speaking, he is quite right. The one billion phone calls made each day is no doubt based on such a feeling. Indeed the original Bell System monopoly was founded on "the expectation of privacy."

And we have only to think of the furor raised by some civil libertarians in having caller I.D. reveal the phone number of the calling party just before the two parties speak. Surely their objection to the electronic equivalent of a peephole in a subscriber's door would not have been made unless it was "felt" that the privacy of their phone conversation was assured. After all, with a wiretap a third party intercepts the conversation and eavesdrops upon *every word.*

Such an unwarranted feeling of security reminds one of the Tooth Fairy and Santa. For, as we know, a teenager with an off-the-shelf-computer linked to the phone network with a modem needs only the current password to tap in a presently technically undetectable manner—remote to any telephone exchange.

A well-known, conscientious West Coast hacker put it this way:

> Any phone line can be listened into from anywhere in the country: The equipment is inexpensive and the technique is known. There is no way for the people on the line to realize they are being monitored. Everybody from your neighbor to Pacific Bell to the Secret Service is vulnerable.

Sanford Sherizen, a Boston-based computer security consultant has a rule of thumb: "If you can communicate out, someone else can communicate in."

Telecommunications privacy, a solution

The American Privacy Foundation (APF), founded in 1975 to achieve "Telecommunication Privacy in the Information Age" hereby proposes just that. Back in February of 1980 [Feb. 28] the long-time Director of MIT's Laboratory for Computer Science, Dr. Michael Dertouzos recommended to the Senate Judiciary "audit trails" as a means of incorporating privacy within the wire and fiberoptic network of point-to-point telecommunications. In fact, the Bell System and AT&T "since its inception" [Cite: AT&T Security Chief William F. Caming, in a letter to Morton Bromfield at Bromfield Corporation dated May 11, 1972] has had an Open Door policy based on subscribers' expectation of privacy. It allows a complaint of phone tapping to be taken up through the ranks to the senior-most telephone official.[1]

The cruel reality of telecommunications privacy today is that it doesn't exist, for a subscriber worth listening to or for anyone else in or out of government. As a litmus test, complain to your phone company about a suspected wiretap, and you will be referred to the Federal Communications Commission. The F.C.C., disclaiming "jurisdiction over wiretapping matters" [Cite: FCC letter to American Privacy Foundation, July 30, 1985], will refer you to the Federal Bureau of Investigation.

The F.B.I.'s Office of Enforcement—having admitted in writing that since at least 1953, no professional tapper has ever been prosecuted [Cite: Letter to American Privacy Foundation from FBI Office of Enforcement, November 17, 1986]—will refer you to the phone company.

Neither the United States nor France nor Britain enjoys telecommunications privacy. Our global village instead shares easy wire tapping. France has its no-admission phone tapping center at the Invalides, Britain at "Tinkerbell Two." During Watergate we all knew that Washington's old Post Office was the tapping center. Today nobody knows.

---

[1] "As a matter of policy within the American Telephone and Telegraph System Companies, any Complaint with respect to a violation of secrecy of communications may be carried by a subscriber to the highest levels of the respective Corporation."

Well, if nobody knows, does anyone care? In a way, yes. Libertarians unwittingly cry out demanding cellular phone protection—though broadcast radio waves are almost impossible to protect.

Is there hope? Well, yes. Protection is indeed possible by using the same basic technology employed by Caller I.D. and adapting it to telephone exchange safeguards. Here is the root for hope as published recently. "U.S. Backs Ending Fiber Optic Export Ban" (The NY Times, Dec. 11, 1993) explains the National Security Agency's interest in the matter:

> The security agency's concern has been that fiber optics, which carry voice conversations and data as pulses of light over hair thin strands of glass are much more difficult to intercept than those carried by radio or satellites.

Washington's best kept secret

Of course the FCC's denial of wire tapping responsibility (which by the way blocked an "en banc" appearance before the FCC's Commissioners) is much like the FAA denying responsibility for air safety. The FBI's non-prosecution of professional wiretappers for forty years or more—while pursuing hackers avidly—is odder still. A non-sinister explanation comes from the pen of John Kenneth Galbraith: "Very often," he wrote, a government agency becomes "the captive" of the very industry it is intended to regulate. In this instance, we are concerned with the business—indeed the industry—of industrial spying. A somewhat sinister explanation comes from an article by David Kahn, the author of the brilliantly written *Codebreakers:* He quotes a Senator's aide, "Let me tap a Senator's phone for three weeks and I will own him."

In my view, whatever federal procedures evolve from these Clipper Chip hearings, trust in Government should be minimized—and for good reason. The relentless history of wire tapping began just 60 years ago with The Communications Act of 1934. It was needlessly crippled by borrowing a non-applicable clause from the Radio Act of 1927, requiring not only proof of interception but also "divulgence." (None of the states has such a requirement.) For 34 years enforcement was made virtually impossible.

Although the 1968 Omnibus Crime Bill removed proof of divulgence, enforcement against the professional tapper continued to languish. Fifteen years earlier, without notifying Congress and without mandatory Notification in The Federal Register, the FBI literally usurped the considerable power to investigate subscriber complaints of wire tapping [Cite: Dial 1.9–8–4]. Vance Packard, author of *The Naked Society,* in finding "incredible evasiveness" at the FCC was moved to comment that the FBI, with phone tapping operations of its own, was hardly the agency to police wire tapping.

The 1968 Crime Bill was *meant to control government tapping.* It wisely had provisions to determine its effectiveness. Four years later the National Wiretap Commission came into being. APF co-founder Harvard Law Professor Vern Countryman, reinforced by the Committee's Chief Counsel Mike Hershman requested permission for expert testimony on the ease of wiretapping through telephone exchanges in slated hearings. The Slated hearings were summarily cancelled. As Professor Sam Dash explained: "It was a phony committee."

Putting relentless tapping in perspective, although an anti-wire tapping device was patented within ten years of Alexander Bell's invention, there has never been a successful government investigation. The closest our government came was in 1985, with Congress' Office of Technology Assessment 1½ year study "Electronic Surveillance and Civil Liberties." Assistant Director Dr. John Andelin, so as to underscore an unprecedented warning to Congress, as its foremost conclusion admitted failure: *"The extent of use of electronic surveillance in the private sector is unknown."*

Fair warning

On January first 1984, despite the submission of similar Invited Comment briefs [under Tunney Act procedures] to Judge Harold Greene by this Foundation and the ACLU in connection with the divestiture of AT&T, a privacy lobotomy occurred. AT&T's Open Door policy—a mere 38 words [See Footnote of Open Door Policy on page two.]—was deliberately excluded from the charters of the regional Bells. On that day, a world recognized futurist's political warning was fulfilled: *"The could plug in your wire whenever the wanted."* [Cite: *1984.*]

Clearly existing tapping control procedures are a charade. (How, for example, did Hoover accumulate 280 file drawers of dossiers [cite: DIAL 1–9–8–4].) Those that distrust contemplated government procedures have ample reasons. One could depict present Court-ordered safeguards as an elaborate massive bank vault door, with the back wall open to the street.

To be sure encrypting is a means of protection: However, the proposals for Clipper provide a "backdoor", which would allow "authorized" government agencies to decrypt supposedly private conversations (voice or data). If the government can use what is in effect a mandatory backdoor, there is the ever-present risk that private parties might also do so by acquiring knowledge of the Clipper technology. Then the government and "private parties" can intercept personal and business transmissions by effectively simply bypassing Clipper's sophisticated encoding.

Is the "cure" worse than the disease? Take for example the massive industrial sabotage waged on Seatrain Shipbuilding, a major corporation building supertankers at the old Brooklyn Navy Yard in the 1970's. In addition to continual disruption of phone communications, their offices were raided time after time, with wholesale lots of office equipment carted off in the night. If there were no master office key, the locks of each and every office would have had to be picked each time. With a master key unlimited easy access was assured. The Clipper Chip works with such an associated Master Key, making access to corporate secrets far simpler.

Clipper does have one "flaw" with respect to "authorized" government decrypting, in addition to flaws highlighted by testimony of others. Near the beginning of a transmission through a Clipper Chip, the encoded serial number of the chip is sent along with the encoded message. A non-government interception cannot read this serial number unless he has the LEAF (Law Enforcement Access Field) key. All Clipper Chips have different serial numbers, but use the same LEAF key. The sophisticated originator gaining access to the LEAF key could easily disguise his serial number so that the government could not obtain the true number and therefore could not obtain the correct Escrow Key to decrypt the transmission. This apparent Achilles Heel would, despite contentions to the contrary, give full unbreached protection to the Key Escrow encrypted transmission. This, it appears, effectively defeats the ability of the government to decrypt an intercepted transmission by a sophisticated industrial spy or criminal.

Two birds with one stone

You will remember that in the Bush administration FBI Director William Sessions initiated a plea to compel all phone companies to incorporate equipment and software to make eavesdropping of telephone and cable networks easier still. As the attached detailed Open Letter suggests, it is not necessary—existing tapping facilities can easily monitor suspected terrorists and drug dealers. What his unexplained, unsupported request does do—and the request is still pending—is to enable illegal trawling or fishing of the massive Main Trunk traffic flashing *between* digitized exchanges—traffic emanating from hi-tech industry, not from targeted drug dealers or terrorists.

Is there really a need for government to require easier still tapping and to in effect mandate unlimited back door access? The track record of 60 years of uncontrolled illegal tapping justifies a resounding no.

U.S. DEPARTMENT OF JUSTICE,
Washington, DC, November 17, 1986.

Mr. MORTON BROMFIELD,
American Privacy Foundation,
Wellesley Hills, MA.

DEAR MR. BROMFIELD: Your September 24, 1986, Freedom of Information Act request, to Mr. Jay B. Stephens has been referred to this Unit for response. In that request, you sought a list of "professional wire tappers" (who engage in industrial espionage and political tapping) prosecuted under Title III and/or The Communications Act of 1934, in the years since 1953.

We have conducted a search of the General Litigation and Legal Advice Section (the section in the Criminal Division most likely to have the record you are seeking.) This section advised that it does not have a list such as you describe nor is it aware of the existence of any such list or information from which such a list could be derived.

Sincerely,

L. JEFFREY ROSS,
Chief,
Office of Enforcement Operations Criminal Division.

FEDERAL COMMUNICATIONS COMMISSION,
Washington, DC, July 30, 1985.

Mr. MORTON BROMFIELD,
Privacy Foundation,
Wellesley Hills, MA.

DEAR MR. BROMFIELD: After discussing your request for a general *en banc* Commission meeting with the Office of General Counsel, and the Chairman's Office, I must inform you that the Federal Communications Commission does not have jurisdiction over matters of wiretapping. As a result of the *Omnibus Crime Control Act of 1968,* Congress clearly placed jurisdiction over wiretapping with the United States Department of Justice.

Due to lack of subject matter jurisdiction, your request for a general *en banc* hearing can not be accommodated.

Sincerely,

WILLIAM A. RUSSELL, JR.,
Director,
Office of Congressional and Public Affairs.

AN OPEN LETTER TO FBI DIRECTOR WILLIAM S. SESSIONS FROM MORTON BROMFIELD ON BEHALF OF THE AMERICAN PRIVACY FOUNDATION

With all due respect, the recent OPED appeal by you "to preserve the ability of law enforcement officers to intercept—to wire tap—conversations of people engaged in serious crimes" is not only unnecessary but harmful to the health of America's hi-tech industrial base.

As you say, "new digital technology spells trouble" —true, but not for the FBI with pre-selected targets. These individuals and small groups can continue to be eavesdropped upon at their local telephone exchange by tapping the terminals of the "twisted pair" of wires leading to a suspect's handset. If the conversation is digitized right up to a target's electronic handset, your agent merely obtains an electronic handset similar to that purchased by the drug dealer. Or your agent merely plugs in an off-the-shelf adapter—a slightly modified Centrex Recording Interface (CRI–376) for under $200 will do—and plain language will result.

Your chief of the Engineering Research Facility at Quantico, Virginia, apparently did not know of these easily obtained countermeasures. It turns out that Mr. James Kallstrom's request for modifying the switchgear of this nation's 100 billion dollar telecommunications industry is not based on any study of his. He explained that the root of this considerably expensive request was a suggestion of an unnamed telephone engineer of an unnamed telephone company.

This nebulous proposal also was made without establishing that the FBI's routine local exchange tapping is in any way threatened. Instead the scenario is that of an agent having to climb a telephone pole, burdened with a huge black box and applying alligator clips. Alligator clip/telephone pole tapping went out with hulahoops.

Separating out the misinformation, the proposal is aimed at a new, unneeded capability of tapping into a phone company's digitized Main Trunk traffic flashing *between* digitized telephone exchanges. Mr. Kallstrom would have such switchgear as AT&T's #5ESS and Northern Telecom's DMS 100 altered so as to facilitate interception—to "port out" so as to segregate and extract transmissions of yet-to-be-identified targets. Such interception is known as "trawling" in England and "fishing" within the States, where it is illegal to fish.

Prior to your stewardship other moves by the FBI in this area were clearly not in the interest of the Bureau itself. While you cite the Omnibus Crime and Safe Streets Act of 1968 as support for this needless proposal, Title III of that Act was intended to control wire tapping by federal officials and put a stop to illegal phone tapping. Legislators wisely made provisions to verily its effectiveness with the formation in 1973 of the National Wiretap Commission. The FBI usurped its investigation, flooding the Commission with erroneous information saying illegal wire tapping is minor, mostly involving marital matters, political tapping (despite Watergate) is one to two percent of the total, and industrial espionage—well, that is nonexistent. An FBI staffer went before the Commission to fully explain this, but his testimony was inexplicably curtailed.

May we suggest the following simple procedure for coping with any future broadening of digitized traffic in connection with court-ordered tapping of suspects: The FBI requests and receives a court order for a phone company to transmit on FBI leased lines all phone traffic sent to a target identified by the court order. This procedure would encompass and catch all call-forwarded traffic. This procedure need not and would not involve any issues of encryption. Finally, this need not and would not distinguish between analog and digital messages.

Query: Is this not sufficient for the FBI's legitimate need?

You could well wonder, Mr. Sessions, that if this procedure will suffice, why then a proposal to facilitate the tapping of MAIN TRUNK traffic? Well, large volumes of digitized voice and data communications emanate from hi-tech multinationals. And contrary to the FBI's "findings" that industrial espionage is nonexistent, we have a recent burst of glasnost from the KGB's Press Service: "industrial espionage is conducted everywhere and this is considered a perfectly normal thing."

But this still leaves a question. Why would the FBI act as a front for the business—indeed the industry—of wire tapping? The answer for this can be found in the words of John Kenneth Galbraith: "Very often," he wrote, an agency "becomes the captive of the very industry it is intended to regulate."

STATEMENT OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association (TIA), which represents more than 550 U.S. manufacturers of telecommunications equipment, wishes to commend Representative Edwards and Senator Leahy, and their very capable staffs, for their efforts to work with representatives of the telecommunications industry to craft legislation to clarify the telecommunications industry's obligations to assist law enforcement authorities in the implementation of court-ordered wiretaps. H.R. 4922 and its Senate counterpart, S. 2375,[1] are the product of a lengthy and reasoned discussion between congressional, law enforcement, and telecommunications industry interests, and these bills represent a significant improvement over FBI Digital Telephony proposals circulated in 1992 and February 1994. Accordingly, while the TIA prefers continued efforts to foster cooperation[2] between law enforcement authorities and manufacturers of telecommunications equipment, the TIA believes that further refinement of H.R. 4922 would yield legislation which accommodates the legitimate needs of the law enforcement community and adequately safeguards the interests of telecommunications equipment manufacturers.

While many of the TIA's concerns regarding the impact of this legislation were addressed during the negotiations which preceded the introduction of H.R. 4922, there remain two issues that the TIA believes require the attention of the Committee.

WHO DEFINES "REASONABLE CHARGE"?

The first matter of concern to the TIA is that of who defines what constitutes a "reasonable charge" for equipment modifications required under Subsection 2605(b). Historically, the price that manufacturers of transmission and switching equipment charge for their products has been determined by market forces, and the price of such equipment traditionally has not been regulated. This reliance on market forces has created a robustly competitive market for the manufacture and sale of telecommunications transmission and switching equipment, and it has encouraged technological innovation by those involved in the manufacturing process.

The Committee should seek to ensure that the present reliance on market forces is not disturbed, and thus should take care, in Subsection 2605(b), to explain that it is not the Committee's intent for the Federal Communications Commission, or any other agency of the federal government, to regulate the price of telecommunications transmission and switching equipment. The TIA regards regulation as unnecessary in what is a truly competitive marketplace, and asks the Committee to clarify that determinations regarding what constitutes a "reasonable charge" for modifications should be made by manufacturers, in consultation with their customers, in accordance with normal and accepted business practices.

Additionally, the TIA urges the Committee to clarify Subsection 2605(b) to clearly indicate that when a manufacturer undertakes "such modifications as are necessary to permit" its customer, i.e., a telecommunications carrier, to comply with the requirements of H.R. 4922, the manufacturer is to be paid by the telecommunications carrier, in accordance with normal and accepted business practices.

---

[1] Hereafter referred to as H.R. 4922.

[2] Such cooperation has been conducted in fora such as the Electronic Communications Service Provider (ECSP) Committee, which is sponsored by the Alliance for Telecommunications Industry Solutions (ATIS).

PENALTIES FOR FAILURE TO COMPLY

The second matter of concern to the TIA is possibility that manufacturers will face civil penalties if they fail to comply with the requirements of H.R. 4922.

Under normal business practices, telecommunications carriers set forth technical requirements (in a request for quotation or RFQ) when they contract for equipment. The provisions of H.R. 4922 are consistent with this practice, as, in accordance with Subsection 2605(a), telecommunications carriers would communicate to their preferred or chosen manufacturer what type of modifications, i.e. intercept capabilities, may be necessary. After such communication, the manufacturer would be compelled, by its existing contract (and, presumably, by its desire to secure future contracts), to provide whatever modifications might be required. The TIA acknowledges and appreciates the bill's reliance upon the existing and accepted process for procurement.

The TIA is much less comfortable, however, with the provisions of Subsection 2607(f), that would subject a manufacturer which fails to provide the necessary modifications to a civil penalty of up to $10,000 per day for each day such manufacturer is not in compliance with the requirements of H.R. 4922. While the imposition of civil penalties may be appropriate with respect to telecommunications carriers which fail to comply with the requirements imposed by H.R. 4922, in that there is no marketplace mechanism to ensure carrier compliance, there is no need to apply such significant penalties to manufacturers, as there is an existing marketplace mechanism to ensure manufacturer compliance.

If a manufacturer fails to comply with the requirements of H.R. 4922, said manufacturer will face significant risk of a breach of contract suit brought by any carrier which employs said manufacturer's equipment and is, therefore, unable to comply with the requirements set out for telecommunications carriers. Given the likely severity of the civil and marketplace sanctions that would accompany a breach of contract suit, the TIA believes that market considerations will adequately ensure manufacturer compliance. Accordingly, the TIA considers the imposition of civil penalties on manufacturers to be both totally unnecessary and counter to the cooperative spirit embodied in H.R. 4922.

In sum, the TIA considers H.R. 4922 to be a significant improvement over previous legislation proposals regarding digital wiretap capabilities, and believes that with the aforementioned clarifications, H.R. 4922 will be a bill that will meet the legitimate needs of the law enforcement community and safeguard the interests of manufacturers of telecommunications equipment.

The TIA thanks the Committee for the opportunity to comment on this important legislation, and looks forward to working with the Committee's members and staff.

STATEMENT OF AT&T CORPORATION

AT&T would first like to extend its gratitude to Senator Leahy and Congressman Edwards for the considerable efforts they and their staff have made during the past several months to draft legislation outlining the telecommunications industry's obligations to assist law enforcement implement court-authorized wiretaps. Their interest and knowledge of and commitment to the public's, telecommunications industry's, and law enforcement's concerns, as reflected in S. 2375/H.R. 4922 (the "Leahy/Edwards bill"), has made progress possible on a number of issues that few thought could be made. They have worked diligently to try to balance the many competing law enforcement, privacy, and technological concerns that are raised by law enforcement's wiretapping needs.

AT&T's interest in the Leahy/Edwards bill arises from the many roles we have in the telecommunications industry. One is as a provider of telecommunication services which are subject to wiretap orders. Another is as the manufacturer of the literally thousands of switches used by a variety of telecommunication service providers, including the local exchange companies and cellular service providers, which will have to be retrofitted to meet the bill's requirements.

Finally, as a company that relies on its good name and customers' trust, AT&T is deeply concerned about this bill and its effect on our customers' privacy rights and expectations. AT&T has always worked to cooperate with law enforcement in a manner that is consistent with the law and the rights and expectations of our customers. AT&T believes that our record on both of these matters is one of which we can be proud—AT&T has a strong record of protecting its customers' privacy and is not aware of any failure on our part of to satisfy any authorized law enforcement request.

AT&T has also been an active participant in the Electronic Communications Services Provider Committee ("ECSPC") since its inception, devoting considerable time and resources to it. ECSPC was formed specifically to address and resolve law enforcement's concerns and, despite the FBI's criticisms of its results to date, AT&T believes that ECSPC has proven to have had considerable merit in addressing law enforcement's concerns. In fact, all parties, including the FBI, acknowledge the need for and usefulness of ECSPC and it has served as the model for cooperation that is established by the bill.

It is important to note that law enforcement's ability to implement wiretaps, though vitally important, is not the only public policy issue affected by this legislation. The core of this bill—how limited resources (both financial and technical) are to be deployed in the telecommunications industry—is also 'at the core of the National Information Infrastructure ("NII"). The public, Congress, and the Administration have all recognized the importance of the NII to virtually every aspect of life and the U.S. economy—education, medicine, job creation, and improved communication for consumers and businesses.

The cornerstone of the NII is the telecommunications industry and its deployment of the greatest number of services as quickly as possible at the lowest possible cost.

These are tremendous demands and are being made at a time when competition in the telecommunications industry is forcing carriers, to be more and more conscious of costs and how best to deploy limited financial and technological resources. AT&T would therefore urge the Subcommittees to continue to narrow and clarify the bill's language so that it achieves its stated purpose without needlessly slowing the deployment of telecommunications services and the advancement of the NII.

NEEDED CLARIFICATIONS

AT&T has been encouraged by the progress that has been made between industry and law enforcement during the past few months towards narrowing the scope of the legislation. Several issues remain, most of which AT&T hopes can be worked out as part of the legislative process and with the agreement of all involved.

There remain, however, two very critical issues which have yet to be sufficiently resolved in the bill. AT&T believes that the failure to clarify these issues could have a chilling effect on the development and deployment of new services and that they need to be resolved. These issues, more fully described below, are (1) will law enforcement compensate carriers for the full cost of compliance with the bill's requirements, particularly those needed to retrofit existing services, and (2) under what circumstances will carriers be able to deploy new services that do not meet the requirements of the bill.

It is essential to industry that the government pay the full cost of compliance with the bill's requirements, especially those needed to retrofit existing services, for a number of reasons, including:

- It will require law enforcement to focus on what they actually require to accomplish their legitimate needs thereby freeing resources they do not actually require for other purposes.
- It will provide an essential mechanism for Congress to control both the costs and level of law enforcement involvement in the development of new services.
- It will ensure that the fewest taxpayer dollars are spent to address legitimate law enforcement concerns.
- It will minimize the competitive disadvantage that carriers covered by the bill will face from persons not covered by the bill.

Law enforcement, as represented by the FBI, has repeatedly indicated their intention to compensate carriers for the full cost of retrofitting their existing services and for meeting law enforcement's ongoing capacity requirements. This intention is *not,* however, fully reflected in the proposed bill. Instead, the bill states that the Attorney General will pay all retrofit costs, but it only appropriates $500 million towards such costs—a number virtually all agree is *significantly* less than the amount needed to fund all of the capability and capacity costs generated by the bill's requirements. The bill indicates that the lack of funding can be considered by a court when determining whether compliance is reasonable, but such lack of funding does not rise to the level of an absolute defense. This leaves carriers with the obligation to meet all of the bill's requirements, but with no guaranteed access to the funding law enforcement has agreed to provide.

AT&T strongly urges the Subcommittees to clarify the bill to reflect law enforcement's clearly stated intention to fund all of the retrofitting and capacity costs. This could be accomplished in the bill either by clearly stating that if the government does not compensate a carrier to retrofit certain services or switches, such carrier shall not be required to meet the bill's requirements with respect to those services or switches, or by appropriating the full amount needed.

With respect to the other costs of compliance (*e.g.,* the cost of the research and development needed to build intercept capability into new services), the FBI has indicated that they will be *di minimis* and can therefore be easily borne by the carriers. Whether such costs are or will remain *di minimis* over time is, however, simply impossible to predict. AT&T would therefore respectfully ask that the Subcommittees include a clear mechanism in the bill by which carriers can be compensated for the costs of their ongoing compliance with the bill's requirements if such costs prove to be more than *di minimis.*

The other area that needs clarification is the section that outlines the circumstances under which carriers can deploy services that do not meet the bill's requirements. Sections 2602 and 2607(c) of the bill indicate that a carrier could deploy such a service if "(1) alternate technologies or capabilities or capabilities or the facilities are not reasonably available to law enforcement for implementing the interception of communications or access to call identifying information; and (2) compliance with the requirements of this chapter is reasonably achievable through the application of available technology to the feature or service at issue or would have been reasonably achievable if timely action had been taken." (emphasis added)

Simply put, this language does not provide clear enough direction for a court as to how it should decide the question of when a service that has an "wiretap problem" can be deployed. Without such clarity and direction, it is impossible to predict how a court would rule on such an issue. This unpredictability, in turn, could have a chilling effect on the development and introduction of new services.

The simple reality is that, the less clear this section is, the more unwilling a carrier will be to allocate increasingly limited resources to the development of a service or feature that may have an a wiretap problem. Before it can prudently invest thousands, and perhaps millions, of dollars on a new service, a carrier must be able to plan and know whether it can be introduced. This "bottom line" should be clear without a carrier having to go through the costly and time-consuming stages anticipated by the bill—research and development, working with standards setting bodies, and a rulemaking procedure at the FCC—or risking court action.

The section-by-section analysis that accompanied the bill gives some guidance on the drafters' intent on this issue. It states,

> "Of necessity, a determination of 'reasonably available' will involve a consideration of economic factors. This limitation is intended to excuse a failure to comply with the capability requirements or capacity notices where the total cost of compliance is wholly out of proportion to the usefulness of achieving compliance for a particular type or category of services or features. This subsection recognizes that, in certain circumstances, telecommunications carriers may deploy features or services even though they are not in compliance with the requirements of the Act." Sectional Summary, p. 7–8.

This language is an important first step, but further guidance is needed in the bill itself. Thus, AT&T would again urge the Subcommittees to clarify this crucial issue in the language of the bill to indicate clearly that features and services may be deployed when the cost of achieving compliance with the bill's requirements exceeds the commercial usefulness of the service or feature in question.

OBLIGATIONS OF MANUFACTURERS

The bill imposes an obligation on manufacturers to provide carriers with the modifications they need to comply with the bill's requirements on a reasonably timely basis. The bill also provides that manufacturers will be paid a reasonable charge for such work, correctly recognizing that manufacturers, unlike the carrier which can recover the costs of its compliance with the bill from the government or its ratepayers, have only one source for compensation for such costs: its customers, the carriers.

In addition, the requirements imposed on manufacturers by the bill mirrors what manufacturers already do for their customers today: consult with them and provide such services and features they request. These obligations, therefore, are in addition to those already imposed on manufacturers by the carriers under the contract they will surely have for the type of equipment (switching and transmission equipment) covered by this bill.

Thus, manufacturers will subject to both a double set of obligations with respect to interception capabilities—if a customer asks AT&T to build intercept capability into its services and AT&T fails to so in accordance with the terms of its contract, it risks court action under this bill and a very costly breach of contract suit. Given this double obligation, AT&T respectfully asks that Congress not impose any additional obligations, financial or legal, on manufacturers.

FBI reporting obligations

Finally, the bill imposes substantial obligations on the telecommunications industry. It is important, as noted above, that these obligations not be imposed unnecessarily. To help ensure this, AT&T would encourage the Subcommittees to include a requirement that law enforcement provide Congress with an annual report on its interception-related and interception-affecting capabilities. In this way, Congress could maintain oversight over these issues, while at the same time minimizing the costs to the telecommunications industry and, ultimately, the consumer.

In conclusion, AT&T would like to again thank Senator Leahy and Congressman Edwards for their leadership and efforts. AT&T looks forward to working with you and your staff through the legislative process in efforts to improve and clarify the bill and to fashion legislation which will best address the legitimate needs of law enforcement, while protecting the customer's privacy and the telecommunications industry ability to speed the deployment of new services.

Statement of MCI Communications Corporation

MCI welcomes this opportunity to express its views on the recently introduced "digital telephony" legislation.

MCI recognizes that S. 2375 and H.R. 4922 represent substantial improvements over the FBI's proposals and we commend Senator Leahy, Congressman Edwards, and their staffs for their leadership in achieving these improvements. In particular, we support the limitations contained in the legislation that exempt interexchange carriers to the extent that their facilities merely interconnect two other carriers.

MCI has several concerns about the legislation that make it fall short of a bill that we could support at this time. Under the proposed legislation, the government commits to pay indefinitely for costs incurred by industry in increasing the surveillance *capacity* of the networks. We believe that the government should also commit to pay indefinitely for costs incurred in increasing the networks' surveillance *capability*. Our main concern is that this legislation will result in the enactment of a largely under-funded mandate. The legislation should ensure that telecommunications carriers not be subject to the new surveillance requirements unless the government pays for the modifications to facilities and services needed to comply.

Thus, MCI strongly supports the Digital Privacy and Security Working Group's proposal to amend the bill to clarify the link between compliance obligations and reimbursement of costs. Under this "pay-as-you-go" approach, telecommunications carriers would be required to comply with the new law's provisions only to the extent that they have been reimbursed by the federal government. This, in turn, will help prevent unnecessary modifications that may otherwise be required to permit digital surveillance.

MCI's interest in digital telephony legislation

Pursuant to the existing requirements of section 2518(4) of Title 18, United States Code, which directs carriers and others to furnish all information, facilities, and technical assistance necessary to accomplish an authorized interception, MCI already cooperates extensively with law enforcement in conducting electronic surveillance. Furthermore, MCI has actively participated in the on-going dialogue between industry and law enforcement conducted within the Electronic Communications Service Providers Committee sponsored by the Alliance for Telecommunications Industry Solutions.

MCI has a direct and material interest in this legislation, which would compliment the existing requirements of section 2518(4). While the local exchange networks may bear the primary responsibility for complying with the new requirements, the interexchange networks remain subject to the bill's provisions. This recognizes that there exist services for which surveillance points cannot be identified in the local exchange network.

Furthermore, while we know of no reports of unsuccessful attempts to conduct authorized surveillance on interexchange networks, MCI's business ventures will increasingly take it into the wireless and the competitive local exchange lines of business. It is in these areas where the majority of incidences of surveillance have traditionally occurred. Therefore, this legislation's requirements are significant to MCI's present and future activities.

GOVERNMENTAL PAYMENT AS A PREREQUISITE TO MODIFYING TELECOMMUNICATIONS FACILITIES

S. 2375 and H.R. 4922 would authorize $500 million to be spent by the Attorney General in reimbursing telecommunications carriers for bringing their networks into compliance with the bill.

At the outset, MCI is *very concerned* that the costs estimates that have been cited are based on surveillance obligations that are not clearly stated in the legislation. These requirements will be refined by the industry standards process and by the FCC. Even when the obligations are reasonably defined, it will take time for industry to identify the technological alternatives that will satisfy those requirements across the various services. Therefore, it is difficult for individual entities to assess the ultimate financial impact to their business operations and, eventually, the ratepayer.

As has been stated by USTA, CTIA, GAO, and others, the true extent of the costs associated with developing and deploying the modifications necessary to existing facilities to satisfy the bill's surveillance requirements is not known. While the FBI contends that $500 million will be sufficient to cover all reasonable industry expenses associated with this bill, even Director Freeh testified in March of 1994 that compliance costs could run to $1.5 billion. Industry estimates put compliance costs at $3 billion or more. As the law enforcement agencies' (LEAs') requirements and industry discussions evolve, a clearer picture of the actual costs should evolve. MCI urges Congress to delay compliance dates until the actual requirements as well as the means to implement those requirements are known.

Clearly it is in the interest of all parties to do what is best for the country at large. A poll reported in *Time* magazine earlier this year found that "two-thirds of Americans said that it was more important to protect privacy of phone calls than to preserve the ability of the police to conduct wiretaps." Thus, Congress should assure the voting public that any measures enacted will continue to protect their rights to privacy, spend their tax dollars prudently, and not create hidden costs by shifting surveillance costs to carriers who will ultimately pass them on to their customers.

The FBI insists that $500 million will suffice to modify the nation's networks to permit necessary electronic surveillance. What happens, however, if the $500 million (or whatever lesser amount is actually appropriated) fails to cover the costs of complying with the government's requirements? Requiring payments as a condition of modifying facilities to comply with the bill's surveillance requirements would have several advantages compared to enacting a largely under-funded mandate:

1) *Efficiency:* Budgetary constraints can prevent the deployment of unnecessary surveillance capability. Only the discipline of tying capability to funding limitations will ensure that law enforcement allocates limited resources in the most efficient manner to obtain surveillance capabilities and capacities when and where they are needed most without burdening industry and, more importantly, other customers with needless costs and delays in access to innovative service offerings.

2) Equity: Taxpayers, not ratepayers or shareholders, should bear the cost of a public good—the greater availability of this investigative tool. Limiting obligations to the extent of government reimbursement spreads the cost of surveillance feature ("a public good") over the entire public as opposed to having common carrier customers "subsidize" improvement of the rest of the public's safety.

3) *Oversight:* The federal government should not hide its electronic surveillance expenditures from public scrutiny. Mandating electronic surveillance without a corresponding funding requirement will distribute costs over the customers and shareholders of common carriers without any visibility to the "public" on whose behalf the costs are being incurred or to their representatives in government. On the other hand, direct payment by the government, using funds appropriated by the Congress, will encourage and facilitate congressional oversight.

4) *Cooperation:* To date, law enforcement and the intelligence community have had a very close, cooperative relationship with common carriers. While mandated to provide "technical assistance," carriers have gone out far beyond the letter of that requirement to accommodate the needs of the government in this area. Imposing onerous requirements on industry without funding needlessly jeopardizes the heretofore positive and productive relationship between industry and law enforcement.

The cost of this surveillance technology to industry does not end with its deployment. The legislation also should commit the government to paying for *operating and maintaining* these government-imposed capabilities. If future needs warrant surveillance of services not covered by the legislation at this time, carriers should be funded regardless of the time elapsed since passage of a bill. Indeed, the government's obligation to reimburse should extend indefinitely, not end after four or six years. The same linkage between reimbursement and compliance in the first four years should be applied to capability requirements in later years.

While we support the "pay-as-you-go" approach and the concomitant need to allocate funds on a priority basis, we note that different carriers will still need funds for infrastructure enhancements to meet the new obligations even if the surveillance capability is not used everywhere. Therefore, the funds need to be carefully and fairly distributed.

To protect the public and industry from unreasonable governmental demands, the lack of appropriated funds sufficient to reimburse telecommunications carriers for modifications and other costs required by the bill should be a complete defense to any claims of noncompliance.

NEW ENTRANTS

We also call to your attention that new entrants in the carrier market must be assured equal funding treatment. Without equitable funding, it will not be possible for those new entrants to compete fairly against established carriers that were granted government funding to develop and implement their surveillance capabilities. Also, government funds should not be made available for carriers to modernize network elements which should have been otherwise upgraded. As noted by GAO at page 7 of its August 11, 1994 report, the government should not pay for "a switch replacement that is needed to meet a capacity requirement [if it] coincide[s] with a switch replacement [needed] to meet a carrier's business needs."

CONCLUSION

In summary, MCI is firmly convinced that choosing the correct funding mechanism is the key to achieving the objectives of the bill most efficiently in the overall public interest. The government should pay for what it demands. Telecommunications carriers should be required to comply with the new law's provisions only to the extent that they have been reimbursed by the federal government. This approach will help ensure that the LEAs' and the public they serve receive the optimum results per dollar spent.

Statement of David A. Banisar, Esq., on Behalf of the Electronic Privacy Information Center

INCREASE IN ELECTRONIC SURVEILLANCE IN 1993

Fueled by an increased use of electronic surveillance by federal officials in drug cases, the number of wiretaps and microphones installed by federal, state and local law enforcement officials increased by 6 percent in 1993 over the previous year. There were also substantial increases in the total number of days in operation, extensions granted and the cost of each surveillance order.

Federal and state courts approved a total of 979 requests, the highest number since electronic surveillance was legalized in 1968. Federal orders increased by 33 percent from 1992, while state investigations decreased by 9 percent. No requests were rejected or amended. In 25 years, only 27 requests have ever been rejected, two most recently in 1988.

Narcotics main offense cited

The vast majority of cases investigated listed narcotics as the primary offense. Seventy-four percent of the federal investigations and 69 percent of all investigations were for narcotics. Racketeering accounted for ten percent of orders and gambling for nine percent. Homicide and assaults accounted for 6 federal cases and 28 total cases. Larceny and theft accounted for 13 cases, loan sharking, usury and extortion for nine more. There was only one case each involving kidnapping and bribery. 48 cases were categorized as "other." The figures continue long-standing trends. Use of electronic surveillance in narcotics cases has increased 240 percent since 1980 and over 500 percent since the legalization of electronic surveillance in 1968. Other offenses have decreased or remained at similar levels.

Federal use increase

Federal investigations accounted for nearly half of all requests for electronic surveillance in 1993. 450 requests were approved by Federal judges, a 30 percent increase in requests over 1992. The 450 requests approved by federal judges represent a 30 percent increase over 1992. Federal use of electronic surveillance has increased nearly 450 percent since 1980. 51 federal judicial districts utilized electronic surveillance in 1993. The Southern District of New York, which includes New York City, and the Eastern District of Michigan, which includes Detroit were the areas with the highest number of orders.

State use of electronic surveillance declines

State use of electronic surveillance declined from 1992 to 526 orders, a decrease of nine percent. State use was at its peak in 1973, when 734 orders were approved. Since the mid-1970's, average number of state orders has fluctuated between 450 and 550 per year.

In 1993, only 23 states used electronic surveillance. New York had the highest number of orders—204.73 percent of state orders were in New York, New Jersey and Pennsylvania.

Total days in use increases substantially

The total use of electronic surveillance methods increased in 1994. Taps and bugs, on average, are in operation far longer overall There was a substantial increase in the total number of days in which surveillance was in reported in operation. The total number of days jumped 22 percent over 1992 to a total of 39,819 total days. Since 1980, there has been a nearly 400 percent increase in the number of days that surveillance devices have been in operation. Federal orders accounted for 56 percent of the days.

Requests for extensions have also increased substantially. The total number of extension requests granted for existing has surveillance increased 27.7 percent over 1992 to 825 total. Since 1980 there has been a 400 percent increase in the number of extensions granted. Each extension was conducted for an average of 29 days.

Costs increase substantially

The average cost of each electronic surveillance order rose sharply in 1993. The average costs increased by 23 percent over 1992, up to an average of $57,000 per order. Federal orders were more expensive, each costing an average of $66,323. The total cost in 1993 for electronic surveillance was an estimated $55 million dollars. Since 1970, the average cost per order has increased 1,100 percent.

Efficiency declines

As the use of electronic surveillance has increased, its efficiency as a law enforcement tool has substantially declined. The vast majority of conversations overhead are determined by the prosecutors to be irrelevant to any investigation. In 1993, prosecutors determined that only 20 percent of all conversations were relevant. For federal investigations, only 17 percent were relevant. These percentages have been rapidly decreasing since the 1970's when prosecutors reported that on average over half of all conversations were relevant.

Prosecutors reported that, on average, 100 different individuals' conversations were intercepted per order. Of the nearly 100,000 people whose conversations were intercepted, 2,400 were reported in 1993 to have been arrested with the assistance of electronic surveillance.

EPIC—ELECTRONIC PRIVACY INFORMATION CENTER

TWENTY-FIVE YEARS OF ELECTRONIC SURVEILLANCE: A STATISTICAL ANALYSIS—REPORT 94–2

EPIC IS A JOINT PROJECT OF THE FUND FOR CONSTITUTIONAL GOVERNMENT AND COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY

Marc Rotenberg, *EPIC Director*

David L. Sobel, *Legal Counsel*

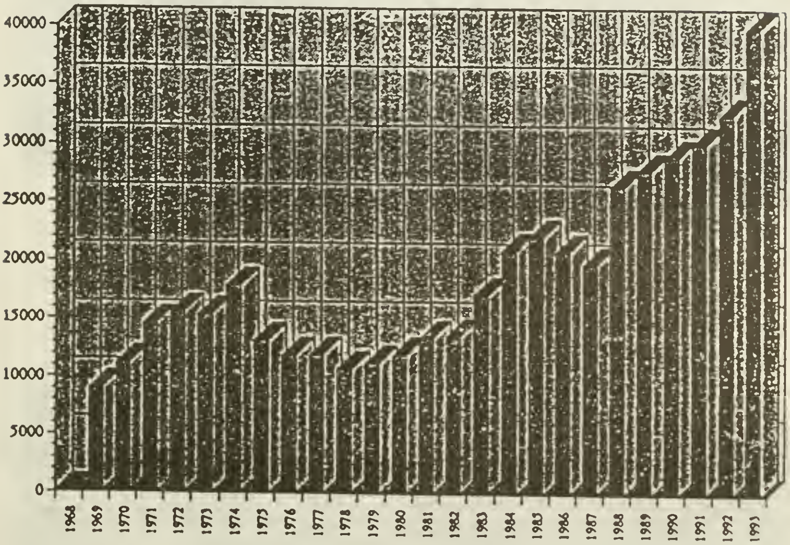
Dave Banisar, *Policy Analyst*

EPIC Board of Advisors:

Hon. John Anderson
Prof. Chris Borgman, UCLA School of Information Science

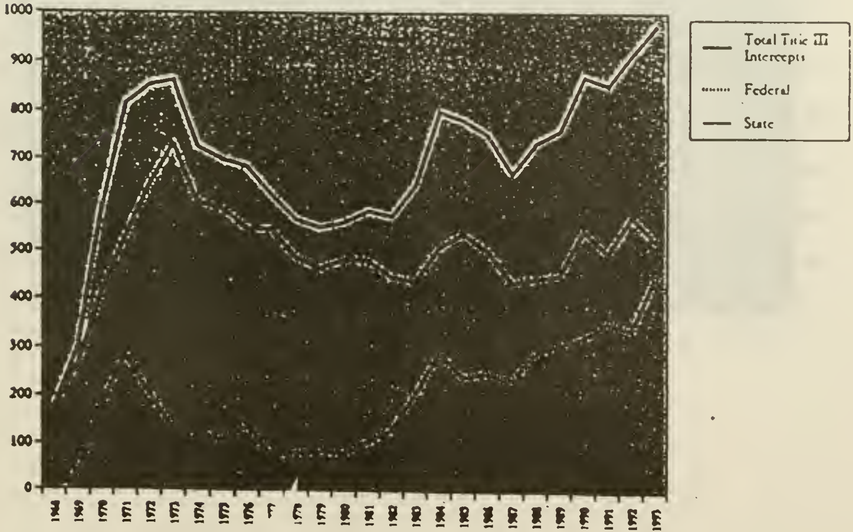
David Burnham, Transaction Records Access Clearinghouse
Dr. Richard Claude, *Human Rights Quarterly*
Simon Davies, Privacy International
Dr. David Chaum, Digicash
Prof. Oscar Gandy, Annenberg School of Communications
Judith Krug, American Library Association
Prof. Gary Marx, University of Colorado Boulder
Dr. Peter G. Neumann, SRI International
Michael Pertschuk, Advocacy Institute
Dr. Barbara Simons, USACM
Dr. Willis Ware, RAND Institute
(affiliations are for identification)

Title III - Total Reported Days in Operation 1968-1993



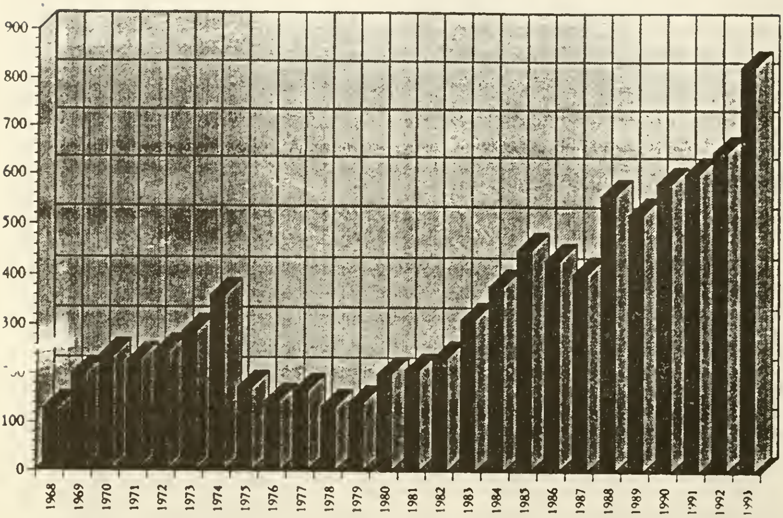
EPIC 1994

Title III Intercepts 1968 - 1993



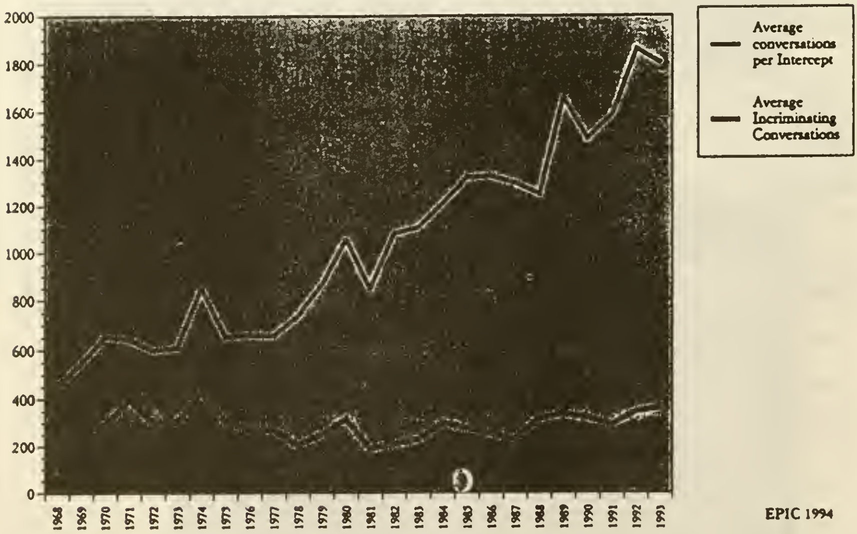
EPIC 1994

Total Extentions Granted 1968-1993



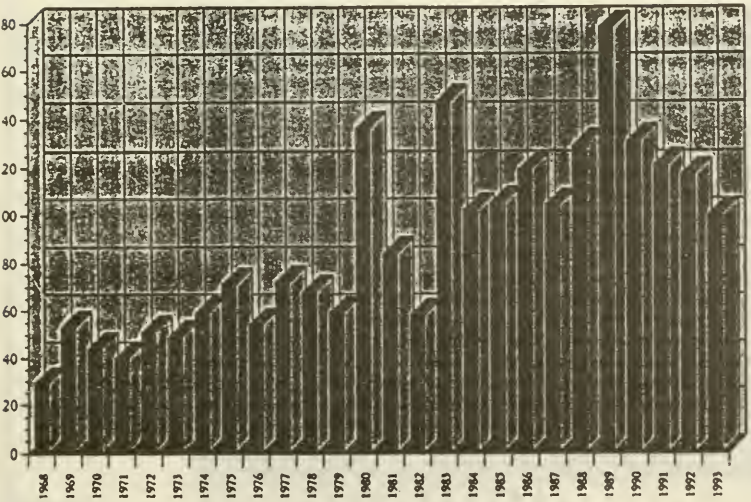
EPIC 1994

Average Conversations and Incriminating Conversations
Intercepted Per Title III Order 1968-1993



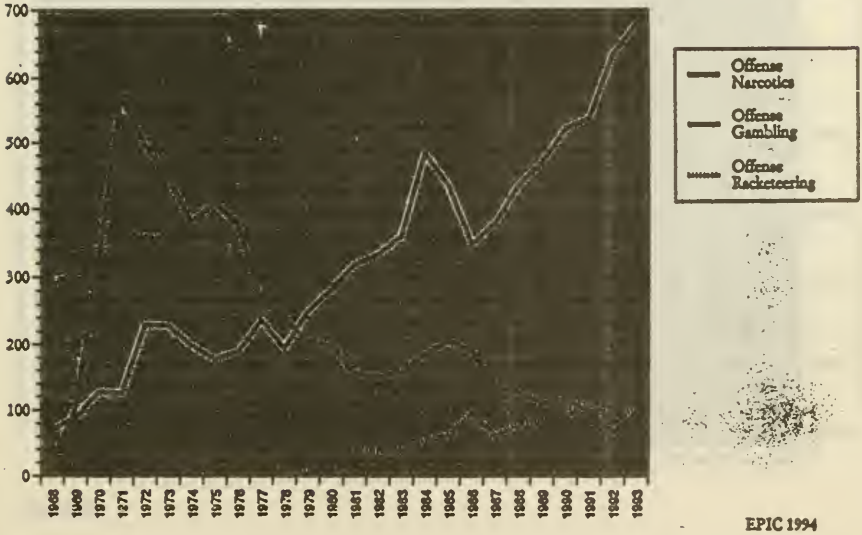
EPIC 1994

Average Number of People Intercepted Per Title III Intercept 1968-1993



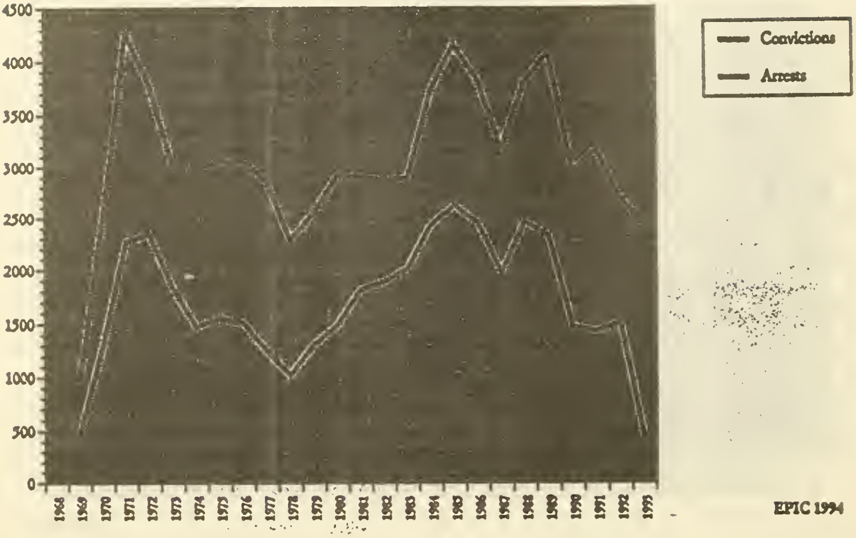
EPIC 1994

Major Offenses Investigated Under Title III 1968-1993



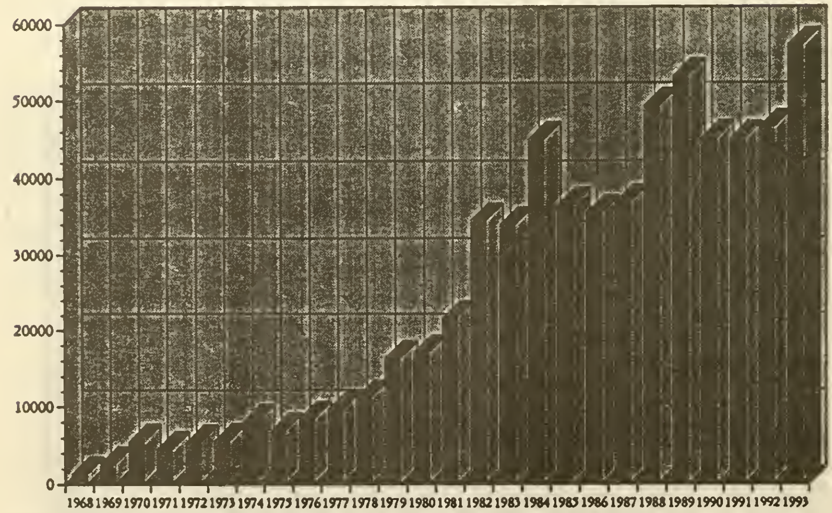
EPIC 1994

Title III Arrests and Convictions 1968-1993



EPIC 1994

Average Cost of Each Title III Intercept 1968-1993



EPIC 1994

AN ANALYSIS OF THE FBI DIGITAL TELEPHONY PROPOSAL

September 18, 1992

This report was prepared by
The Electronic Frontier Foundation
in coalition with:

abcd - The Microcomputer Industry Association
Advanced Network & Services, Inc.
Agson, Inc.
American Civil Liberties Union
Arrow
AT&T
Business Software Alliance
Cellular Telecommunications Industry Association
Computer and Business Equipment Manufacturers Association
Computer and Communications Industry Association
Computer Professionals for Social Responsibility
Digital Equipment Corporation
Eastman Kodak
Electronic Mail Association
Graphics Technologies, Inc.
IBM
Information Industry Association
Information Technology Association of America
Iris Associates
Logistics Management, Inc.
Lotus Development Corporation
Merisel, Inc.
Micro Computer Centers Inc.
Microsoft Corporation
Okidata
Oracle
Panamax
P C Parts Express
Prodigy
Seneca Data Distributors, Inc.
Software Publishers Association
Sun Microsystems
Telecommunications Industry Association
United States Telephone Association
Westbrook Technologies

Executive Summary

Although the FBI has characterized its proposed "Digital Telephony" legislation as relating to the preservation of government's ability to engage in authorized wiretapping, the proposal actually requires that all communications and computer systems be designed to facilitate interception of private messages, on a concurrent and remote basis — thus imposing new engineering standards that go far beyond any existing law. As currently drafted, the proposal would impose substantial costs and create significant uncertainties, despite the absence of any clear showing that the proposed measures would be either effective or necessary. In addition, the proposal raises serious security and privacy concerns.

Beginning in 1991, the FBI expressed concern that technological changes occurring in the telecommunications industry might have an adverse effect on the ability of law enforcement officials to conduct lawful, authorized wiretapping. For example, the FBI raised questions about its ability to extract individual telephone calls from multiplexed signals sent over light fibers using new digital protocols. Various FBI proposals have generated concern on the part of industry that the security and privacy of electronic communications and computer systems might be weakened and that the competitiveness or technical advancement of various systems might be undercut. No one in industry challenges the FBI's right to cooperation in seeking to implement wiretaps or disagrees with the proposition that law enforcement officials need communications interception tools to do their vital job. The communications industry, network users and public interest groups are concerned with the sweep of the FBI's draft proposal and the potential uncertainties and costs it would impose.

Although the FBI proposal is described as relating to "digital telephony," it actually applies to all forms of communication, including all computer networks. The proposal requires that equipment be designed to give access to communications on a "concurrent" basis, regardless of the mobility of a target, in isolation from messages being exchanged by any other persons. These requests may have complex and differing application in different contexts, but they would certainly introduce additional costs and uncertainties for both equipment manufacturers and everyone who offers messaging service to others. These days, the list of those covered by the proposal ("providers of electronic communications services" and "PBX owners") includes just about everyone. Because the wiretap statute was written to protect the privacy of a broad range of communications types, and because of the growing interdependence and intermixing of all forms of communications, the statutory language of the FBI proposal could turn out to require redesign or expensive alteration of:

- *public electronic mail systems, like those offered by MCI, AT&T and others;*
- *all telephone switches and the equipment used by long distance carriers;*
- *software used by online information services like Prodigy, GEnie, Compuserve, America Online and many others;*
- *local area networks, linking all kinds of computers, operated by small businesses, colleges and universities and other organizations, including links into these systems from homes and offices;*
- *PBXs owned by small and large businesses;*
- *high speed networks connecting workstations with mainframes and supercomputers, as well as those carrying traffic across the "Internet;"*
- *radio-based and cellular communications systems, including pocket telephones and computers with radio-based modems;*
- *the thousands of personal computers owned by businesses, hobbyists, local governments, and political organizations that communicate with others via computer bulletin boards;*
- *private metropolitan wide area communications systems used by businesses such as large banks;*
- *satellite uplink and downlink equipment supporting radio and television transmissions and other communications and*

While the FBI proposal is described as relating to "digital telephony," it actually applies to all forms of communication, including all computer networks.

- *air-to-ground equipment serving general aviation and commercial aircraft.*

The United States is becoming an information economy. Imposing mandatory system design requirements on those involved in the transfer of information has an impact on large numbers of people and most sectors of the economy.

There is no doubt that evolving technologies will challenge law enforcement officials and industry alike. We need effective law enforcement tools, as well as appropriate levels of privacy and security in communications and computer systems. The goals underlying the FBI proposal are valid and important ones. But they may well be best achieved without additional legislation. Industry has historically cooperated with law enforcement and is presently engaged in ongoing discussions to identify specific problems and concrete solutions. This cooperative process will lead to needed exchanges of technical information, better understanding on all sides of the real policy issues, and better, more cost-effective solutions. Congress should reject the FBI proposal and encourage continuing discussions that will lead to more specific identification of any problems and to more concrete, cost-effective solutions.

The Digital Telephony Report

Introduction: What Is Proposed?

The most recent FBI proposal imposes obligations to provide various generic interception "capabilities and capacities" and empowers the Attorney General to grant exemptions, after consultation with the Federal Communications Commission, the Department of Commerce and the Small Business Administration. Any person who manufactures equipment or provides a service that does not comply with the broad and vague requirements of the proposed statute would be subject to a civil penalty of $10,000 per day.

How Serious Is the Problem?

The predicate for the FBI proposal is that advances in technology have made it more difficult for the government to intercept particular telephone conversations in the course of legally-authorized wiretapping. There have been few actual problems, historically, in executing authorized wiretaps. None have stemmed from characteristics of communications equipment design (as distinct from limitations in equipment capacity). On the other hand, it is clear that changes in the technologies used for communications will require the FBI (and the communications industry as a whole) to use new techniques and to acquire additional equipment and skills. Some developments, such as encryption, may make interception (or, at least, understanding the contents of what has been "intercepted") much more difficult — but in ways that are not even addressed and cannot be fixed by the proposed legislation. (It is difficult to evaluate the FBI argument that it would have asked for more interceptions if some technological barriers had not existed. There have always been and will always be some technological barriers to interception of the content of communications the participants seek to protect.)

Existing law requires all companies providing electronic communications services to cooperate fully with lawful requests from the FBI and other law enforcement officials — and there is no history of any general failure to provide such cooperation.

Existing law contemplates that the government will bear the costs imposed by requests for access to communications. (As noted below, the proposal does not specifically extend that principle.) There is no showing that the

There have been few actual problems, historically, in executing authorized wiretaps. None have stemmed from characteristics of communications equipment design....

government lacks the financial resources to modernize its communications equipment or to fund the costs of lawful interceptions that it initiates.

Since the total number of content wiretaps in 1991 authorized by Federal and State courts was only 856 taps (and almost 60% of these were at the State level, 356 Federal versus 500 State), and since the call-set-up or pen register tap orders for 1991 at the Federal level were only 2,445, (thus, implying a national total under 7,000), it appears the costs may be better targeted to the specific lines or ports necessary, instead of burdening all lines or ports existing in the network

By comparison, there were over 138 million access lines as of December 31, 1990 according to the United States Telephone Association, and this does not include ports used for cellular or many other network accesses. (We under stand the current FBI budget provides for $9 million for new digital telephony interception equipment.) Thus, although there is valid reason to be concerned that changes in technology will challenge law enforcement agencies to find and adopt new techniques, there is no immediate crisis requiring swift action.

Broad Scope of the Current Proposal.

The FBI proposal covers all providers of "electronic communications services" and all "private branch exchange operators" (PBXs). These days, that means just about everybody, including every business that has its own phone switch and every company that operates its own local or wide area computer network. The Electronic Communications Privacy Act defines "electronic communications services" to include electronic mail, file transfers over a Local Area Network ("LAN") and, indeed, every form of transmission of a message other than voice telephone calls (which are also covered by the proposal as "wire" communications) and sound waves in the open air (the only form of communication not covered by the proposal). *(See 18 U.S.C. 2510(12),(15).)* All "providers" of such services would be affirmatively required, within three years, to provide law enforcement officials with the "capability and capacity" to intercept communications. This capability would have to be provided "concurrently" with the communication, without detection (apparently without regard to the target of the wiretap possibly employing sophisticated wiretap detection capabilities), exclusive of any communications between other parties, regardless of the mobility of the target, and without degradation of service.

These absolute requirements might not be capable of being met, as a technical matter, in some contexts, regardless of costs. The proposal is redundant, in the sense that it requires the ability to access communications at all points during their transmission, even though access at one point is all that is needed in any given circumstance. Although current wiretap law requires "minimization" and use of wiretaps as a "last resort," the proposal imposes obligations on all communications systems as if preserving the ability to wiretap at any point should be the system designer's highest priority. The application of these requirements would have substantially different costs and other implications depending upon where in a communications pathway they were actually applied. In any event, they dramatically expand the nature and reach of current law — which requires cooperation but does not grant the government a right to redesign the communications network or the equipment used by large numbers of businesses.

The FBI has defended its proposal on the ground that it is only seeking to "preserve the *status quo*," by preventing changes in technology from taking away capabilities that Congress meant to assure when it passed the 1968 and 1986 wiretap statutes. But that mischaracterizes the "*status quo*." The current wiretap statutes take the communications networks as they find them and do not require any provider of communications service to redesign the system, or to refrain from using any particular technology, solely on the ground that such a technology would make interception more difficult While there may well be

[The proposal] greatly expands the jurisdiction of the Attorney General and would represent a giant step beyond current law and congressional intent going back to 1968.

sound reasons for all concerned to cooperate to seek to preserve for the government a practical ability to engage in authorized wiretapping, there is simply no existing legal authority for law enforcement officials to mandate the use of particular technologies and, thus, contrary to the claims made by the FBI, the proposal does not simply maintain the *status quo*, but greatly expands the jurisdiction of the Attorney General and would represent a giant step beyond current law and congressional intent going back to 1968.

While the proposal imposes substantial uncertainties, there is no question that, as drafted, it would have an extremely broad reach. As a result, it could complicate the development of various new technologies. Even though the language of the proposal would extend to cable information systems and Automated Teller Machines ("ATMs"), the FBI has stressed in its proposal that various systems might be exempted by executive action. But the exemption authority is vague and standardless — so the net effect is that every system provider has to worry on a continuing basis about whether or not its system is covered. Moreover, the proposal is clearly designed to cover any system facilitating two-way conversation, regardless of the size of the communications service provider. In consequence, any small business that installs its own local PBX system for forwarding calls from customers could be required to replace its equipment with new switches that meet the law's requirements. If current online information services do not track the "services" and "features" used by those who send messages through their electronic mail channels, then expensive modifications might be mandated. Because these electronic mail systems are all being joined together, and some function as links that forward messages between other systems, all might have to be designed to allow "real time" interception by retransmission to a remote site — even though delayed searches of stored files would seem to make a lot more sense in the context of electronic mail.

Costs Likely to Be Imposed by the Proposal.

The costs imposed by this proposal would be passed on to consumers and all subscribers to electronic communications services. The total costs, including costs imposed by its potentially disruptive impact on planning for new computer and communication technologies, cannot be fully assessed — but would be very substantial. In its report on the FBI's proposal, the General Accounting Office ("GAO"), page 1, stated: "*[N]either the FBI nor the telecommunications industry has systematically identified the alternatives, or evaluated their costs, benefits, or feasibility.*" And further at page 4 of the GAO Report: *[T]he [FBI's] May proposal does not address what the telecommunications industry would need to do to be in full compliance with the proposal in the event it is enacted, the meaning of certain technical terms, or who would pay for the cost of wiretapping solutions.*"

Although there is valid reason to be concerned that changes in technology will challenge law enforcement agencies to find and adopt new techniques, there is no immediate crisis requiring swift action.

The proposal mandates compliance with very broadly stated functional standards and contemplates that exemptions (available from the Attorney General, without the benefit of any specific standards or criteria) will be granted only after this broad new governmental authority has been enacted into law. The most recent proposal assumes that the costs of compliance will become a cost of doing business imposed on all communications service providers — and passed on to telephone ratepayers and other subscribers to electronic communications services. (The current law's provision that the government will pay reasonable expenses incurred in cooperating with a specific request for interception has not been expressly applied to this new requirement to "provide the capability and capacity" to respond to such requests.) Communication service providers and computer equipment manufacturers could suffer major losses as a result of delays, mandatory redesigns, and even prohibition of certain technological options. There has been no opportunity as yet to compare (1) the costs the FBI would incur to modernize its approach to interception (especially given the data on the small number of taps performed annually) with (2) the costs that would be incurred by consumers as a result of mandatory limitations on new technology design applied to all technologies nationwide.

Uncertainties Created by the Proposal.

By attempting to establish open-ended duties, broadly defined, in statutory language, the current proposal creates substantial uncertainties and could cause controversy to supplant cooperation. For example, although current interception orders predominantly relate to voice communications, the draft proposal covers all forms of communication. This approach could sweep up systems ranging from the cellular pager to the high-speed network designed to transfer digital data between supercomputers. It raises a wide variety of questions:

- What exactly are the boundaries of the "public switched network" to which the proposal refers?
- On what basis would the Attorney General choose, or be required, to provide exemptions?
- How would the proposal affect systems that regularly encode messages at the point of origin?
- Does the required provision of capacity to intercept "concurrent with the transmission to the recipient" mean that an electronic mail or voice mail or facsimile mail system must be designed to signal the system operator every time a message from a target of an investigation is accessed by the person to whom that message might have been addressed?
- Will it be technically feasible to detect and separate just those parts of a communication signal coming from a particular residence or other source, that "exclusively" represent the content coming from a particular individual?
- What is meant by the new, broad requirement that the government be told what "services, systems, and features" have been used by the subject of the interception?
- Does the required provision of interception capacity "notwithstanding ... the use by the subject ... of any features of the ... system" have the effect of requiring the system provider to offer to defeat any encryption mechanism it may provide to subscribers?
- Does the requirement to provide interception despite the target's mobility mean that systems that inherently allow users to send and receive from multiple points, without notice, cannot be used at all?
- Will it be physically possible or economically feasible to prevent "degradation of services" if the functional requirement for real time tracking of any target means that some central database must be checked by the service provider's computers every time a communication is made?

We don't know the answers to these questions, despite their importance. More importantly, the answers to key policy questions may differ substantially depending on what particular technology and interception need (and minimization goal) is being addressed. And we don't even know by what means providers of electronic communications services and designers and users of electronic communications and computing equipment will find out how the requirements will be applied to their systems. In short, the FBI's proposal, as currently drafted, may generate new and unnecessary controversy, despite its legitimate goals, by attacking perceived problems at the wrong level of generality.

As drafted, the proposal appears to threaten U.S. interests in international trade and competitiveness.

Threat to Security and Privacy.

Ironically, in addition to creating uncertainty and imposing costs, the proposal would itself create new and serious security risks and undermine the privacy of electronic communications. If electronic communications service providers must design their systems to allow and ensure FBI access, then the resulting mandatory "back doors" may become known to and be exploited by criminals. Business is currently attempting to achieve greater security in its communications, to counter the threats posed by unauthorized access, computer viruses, and electronic theft. A proposal the FBI seeks to justify in terms of law enforcement could well have the effect of facilitating violations of law and reducing or preventing effective security measures.

Threat to International Trade and Security Interests.

As drafted, the proposal appears to threaten U.S. interests in international trade and competitiveness. Potential purchasers abroad may not buy products or systems that they know have a "trap door" the United States Government can easily open. If U.S. manufacturers of communications systems and equipment and computer software have to go through a bureaucratic certification or clearance process that is not applicable to their foreign competitors, their race to the market with new technologies will be slowed and their products and designs will be disadvantaged.

Legitimate Law Enforcement Concerns Should Be Served.

There is no doubt that authorized wiretapping is an important weapon properly used by the FBI to fight serious crime. And there is general agreement among communications service providers, and the makers of communications and computing equipment, that the FBI is entitled to full cooperation in its efforts to exercise the powers granted to it in the wiretap statute. If new technologies require changes in police tactics, then accommodations may be needed on all sides to make sure that new tactics that do not threaten the effectiveness or safety of law enforcement (or unreasonably threaten privacy interests) are available. The FBI proposal has served a valuable purpose in drawing attention to the need for adequate planning and redoubled cooperative efforts.

It Is Too Soon to Know if Legislation Will Be Necessary.

Despite the good intentions underlying the FBI proposal, there is certainly no demonstrated need to hamper U.S. technological advances, harm the competitiveness of the U.S. communications or computer industries, or hinder efforts by business to increase computer security, just to make sure that law enforcement officials can continue indefinitely to use the same equipment and procedures that were appropriate for an earlier technology. There has as yet been no clear showing that the design of new technologies will not permit reasonable, affordable and effective techniques to be used for authorized interception. There has been no showing that the industry will not or cannot cooperate fully, share technical information under appropriate protections, and even design and supply new equipment at reasonable cost, insofar as these steps prove necessary for the FBI to accomplish its mission. There has been no clear showing that any capacity limitations could not readily be remedied with the provision of adequate financing for government law enforcement operations.

Congress should reject the FBI proposal and encourage continuing discussions....

The Proposal Is Premature in Light of Industry Efforts.

An ad hoc coalition of interested parties has joined together to study the issues posed by the FBI's proposal and to begin discussions involving various business interests, public interest groups, the law enforcement community, legislative staff, and representatives of the Administration. All involved recognize that the FBI is entitled to have adequate tools to fulfill its law enforcement objectives. For its part, the FBI has recognized the value of industry cooperation and the need for a more robust exchange of technical information. Once the technical issues come into focus, particular policy issues may be ripe for decision, in a context in which the costs and implications of such decisions for trade, security and privacy concerns will be much more clear. Technical Working Groups representing both the telephone companies and the computer industry are hard at work — but the issues are complex and even the first stage of identifying serious potential problems for law enforcement will take some time. Consideration of proposed solutions should await the results of these detailed and technical discussions.

Conclusion.

As the broad collaboration that accompanied consideration of the 1986 amendments to the wiretap statute showed, the public interest in sound law enforcement, and public expectations of privacy and security, are best served by encouraging a constructive exchange of views among industry, concerned citizens and government before any new legislation is enacted. Congress should reject the FBI proposal and encourage continuing discussions that will lead to more specific identification of any problems and to concrete, cost-effective solutions.

For further information contact:

John Podesta, Coalition Legislative Counsel (202) 544-6906
David Johnson, Coalition Counsel (202) 663-6722
Jerry Berman, EFF Washington Office Director (202) 544-9237

Prepared by:

Electronic Frontier Foundation
Washington Office
666 Pennsylvania Avenue, SE,
Suite 303
Washington, DC 20003
(202) 544-9237 tel
(202) 547-5481 fax

U.S. DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION

SUMMARY

Advanced telecommunications technologies threaten to cripple the government's ability to protect the nation against the worst and most dreaded crimes.

The Problem: When in widespread use, the technologies will make it virtually impossible for federal law enforcement agencies to use court-approved electronic surveillance.

The Answer: Congress must enact legislation requiring that the new technologies contain capabilities allowing the government to continue using this invaluable tool to safeguard the United States.

More than 25 years ago, Congress passed a law allowing court-authorized surveillance, and it has become one of the most valuable law enforcement techniques against the very worst crimes.

For example: From 1982 to 1992, more than 22,000 convictions resulted from 8,300 court-approved surveillances.

Without that tool, law enforcement's ability to protect the public will be permanently eroded and the national security will be gravely endangered.

Court-approved surveillance is the most important and often the only way. to prevent or solve life-and-death crimes.

How grave are those crimes?

They appear often enough in newspapers and television broadcasts: Terrorism, espionage, other foreign threats, violent crime, organized crime, drug trafficking, kidnapping—and more.

In addition to the federal government, state and local law enforcement agencies also will be unable to carry out court-approved surveillance because of the new technologies.

That is why the nation's most important-law enforcement organizations at the state and local level also firmly support protective legislation by Congress. They include the International Association of Chiefs of Police, the National Sheriffs Association, the National Association of Attorneys General, and the National District Attorneys Association.

Law enforcement at the grass roots throughout the nation and federal law enforcement stand together on this issue. Their goal is to better protect the people of the United States from harm.

But even now, "digital telephony" is developing so rapidly that several hundred court-authorized surveillances already have been prevented by new technological impediments associated with advanced communications equipment.

New legislation would not endanger privacy rights. The government would be given the same surveillance authority it has had since Congress created the surveillance law in 1968.

Telephone companies and others would only be required to assist law enforcement as they have for the past quarter-century—only now it would be assistance concerning new, different technology.

Without legislation, the government will eventually become virtually helpless to defend the nation from both foreign and domestic threats.

The threats include terrorists with bombs, spies who steal our most sensitive secrets, traffickers importing vast amounts of drugs, kidnappers who prey on children, murder plots, and other grave violent crimes.

Congress must pass legislation that would by reasonable steps allow law enforcement to carry out court-approved surveillance despite the intricate new communications technology and equipment.

Otherwise, the nation will find itself facing even worse crime and national security problems—not only in the rest of this century but well into the next. Failure to act now will cause lasting problems for the safety and security of the American people.

INTRODUCTION

This report by the Federal Bureau of Investigation discusses a major new problem facing the criminal justice system nation-wide: Advances in telecommunications technology that will make it virtually impossible for law enforcement agencies to conduct court-authorized electronic surveillance.

For the benefit of members of Congress and other public officials, the report contains a summary of the key matters involved in the "digital telephony" issue and proposes legislation that would enable law enforcement to conduct court-approved surveillance of communications systems containing the complex new technology.

The draft legislation is titled: "Digital Telephony and Communications Privacy Improvement Act of 1994." It is included in the report along with a section-by-section analysis and other material.

For additional information, please call the FBI's Office of Public and Congressional Affairs, 202–324–2727.

QUESTIONS AND ANSWERS

Question 1. Why do we need legislation now? Is there really a problem?

Answer. For nearly a decade, law enforcement has been encountering technological impediments to court-ordered electronic surveillance. As a result, a number of court orders have been frustrated in whole or in part. These impediments result from the deployment of advanced telecommunications systems which were designed without consideration for law enforcement's interception needs. These impediments prevent or hinder telephone companies from providing law enforcement with the access required to obtain the content of communications that are the subject of court orders. Over the last four years, the government has sought to obtain, without success, a firm commitment from the telecommunications industry to remove the impediments at a fixed, reasonable date in the future. Consequently, legislation is necessary to resolve this impasse. Further delays in correcting these technological impediments will unnecessarily jeopardize the personal safety and economic well-being of the American public. The longer the delay, the bore expensive it will be to correct this serious problem and the longer society will be put at risk and effective law enforcement hampered.

Question 2. Won't the removal of these impediments make the networks less secure and vulnerable to hackers, etc.?

Answer No. As with other specialized services and features included within the telecommunications networks, proper planning and design will ensure the integrity and security Of the net works. Telephone companies already employ techniques which maintain system security and guard against network vulnerability. Removal of the impediments to court-authorized electronic surveillance can be accomplished in a manner consistent with strong systems security. In fact, the legislation contains a network security provision. We are confident that the telephone companies will continue their substantial efforts to prevent "hackers" and others from penetrating the telecommunications networks. Further, since such penetration efforts are considered serious crimes by the Federal government, they will continue to be prosecuted to the fullest extent of the law.

Question 3. Won't this legislation increase wiretapping?

Answer. No. Existing Federal law prescribes a rigorous procedure which law enforcement must follow in order to obtain judicial authorization to conduct electronic surveillance. The proposed legislation does not change the legal requirements or the administrative procedures for obtaining a court order for electronic surveillance, nor does it alter the criminal penalties for unlawfully intercepting communications. The essential purpose of the legislation is to clarify the nature and extent of the existing statutory obligation of telephone companies to provide law enforcement with "the technical assistance necessary to accomplish the interception."

Question 4. Who will pay for removing the impediments?

Answer. The Federal government. The government recognizes that there will be costs involved with preserving the public safety, society's economic well-being, effective law enforcement, and the national security through law enforcement's ability to conduct court-ordered electronic surveillance. The proposed legislation makes it clear that the Federal government will compensate telephone companies for fair and reasonable costs incurred by them during the compliance period established in the legislation.

Question 5. Does law enforcement really need to do wiretaps? Can't it get the same information from other sources?

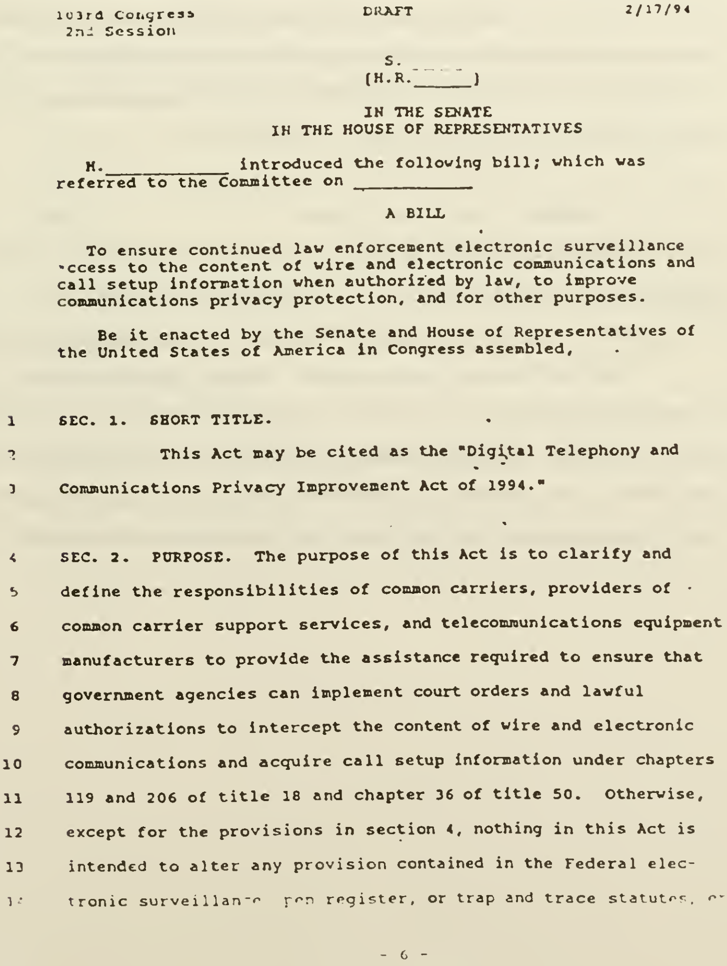
Answer. Court-ordered electronic surveillance is a critically important and unique law enforcement investigative technique. In fact, the law only permits the use of court-ordered electronic surveillance when other investigative techniques will not suffice or are too dangerous. Although other investigative techniques are important, the use of electronic surveillance provides law enforcement with information and evidence that, as a rule, are unobtainable through other investigative techniques.

Question 6. How many wiretaps does law enforcement conduct in a year?

Answer. Under the statutes that permit electronic surveillance in criminal matters, the combined number of electronic surveillance court orders executed in recent years by all Federal, state, and local law enforcement agencies has averaged around 800–900 per Year. The effectiveness of this technique is noteworthy. Between 1982–1992, over 22,000 dangerous felons have been convicted as a direct result of executing some 8,300 court orders for electronic surveillance. Importantly, hundreds of lives have been saved, and thousands of criminal acts prevented, through the use of this critically important technique. Additionally, the economic benefit derived by law enforcement and society as a whole from the use of electronic surveillance (i.e., fines, recoveries, restitution, and economic loss prevented) is in the billions of dollars.

Question 7. Won't this legislation affect our telecommunication industry's competitiveness?

Answer. No. By its very nature the legislation will ensure fairness, equal treatment, and a "level playing field" within the telecommunications industry by requiring all telephone companies operating in the U.S. to remove the impediments to electronic surveillance within three years. Further, similar governmental initiatives are now under way in a number of foreign countries that are designed to maintain the electronic surveillance capabilities of law enforcement in those countries in use against drug cartels, organized crime, and terrorist groups. Thus, as the U.S. telecommunications industry, including equipment manufacturers and support service providers, meet their domestic responsibilities under this legislation, they will be in an excellent position to respond to new market opportunities abroad in meeting foreign law enforcement's electronic surveillance needs.



103rd Congress
2nd Session

DRAFT

2/17/94

S. ____
[H.R.______]

IN THE SENATE
IN THE HOUSE OF REPRESENTATIVES

M.____________ introduced the following bill; which was referred to the Committee on ___________

A BILL

To ensure continued law enforcement electronic surveillance access to the content of wire and electronic communications and call setup information when authorized by law, to improve communications privacy protection, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 1. SHORT TITLE.

This Act may be cited as the "Digital Telephony and Communications Privacy Improvement Act of 1994."

SEC. 2. PURPOSE. The purpose of this Act is to clarify and define the responsibilities of common carriers, providers of common carrier support services, and telecommunications equipment manufacturers to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information under chapters 119 and 206 of title 18 and chapter 36 of title 50. Otherwise, except for the provisions in section 4, nothing in this Act is intended to alter any provision contained in the Federal electronic surveillance, pen register, or trap and trace statutes, or those of any state or other jurisdiction. In particular, nothing herein is intended to enlarge or reduce the government's authority to lawfully intercept the content of communications or install or use pen register or trap and trace devices, or to increase or decrease any criminal penalties for unlawfully intercepting the content of communications or installing or using pen register or trap and trace devices, or to alter the provisions regarding service provider assistance, payment for assistance, causes of action, civil liability, or good faith defenses.

The Act is further intended to improve communications privacy protection for cordless telephones, certain radio-based data communications and networks, communications transmitted using certain privacy-enhancing modulation techniques, and to clarify the lawfulness of quality control and service provision monitoring of electronic communications.

SEC. 3. COMMON CARRIER ASSISTANCE.

(a) New section. Chapter 109 of title 18, United States Code, is amended by adding the following new section:

"Sec. 2237. Common carrier assistance to government agencies.

"(a) **Assistance requirements.** Common carriers shall be required to provide forthwith, pursuant to court order or lawful authorization, the following capabilities and capacities in order to permit the government to conduct electronic surveillance and pen register and trap and trace investigations effectively:

"(1) The ability to execute expeditiously and simultaneously within a common carrier's system all court orders and lawful authorizations for the interception of wire and electronic communications and the acquisition of call setup information related to the facilities or services of subscribers of such common carrier;

"(2) the ability to intercept the content of communications and acquire call setup information concurrent with the transmission of the communication to or from the subscriber's facility or service that is the subject of the court order or lawful authorization, to the exclusion of any wire or electronic communication or call setup information of any other subscriber, notwithstanding the mobile nature of the facility or service that is the subject of the court order or lawful authorization or the use by the subscriber who is the subject of the court order or lawful authorization of any features offered by the common carrier;

"(3) the ability to intercept the content of communications and acquire call setup information unobtrusively and with a minimum of interference with any subscriber's telecommunications service; and

"(4) the ability to receive, in a generally available format, the intercepted content of communications and acquired call setup information at a location identified by the government distant from the facility that is the subject of the interception, from the interception access point, and from the premises of the common carrier (except where emergency or exigent circumstances such as those described in 18 U.S.C. 2518(7), 2518 (11)(b), or 3125, or in 50 U.S.C. 1805(e), necessitate monitoring at the common carrier's premises).

"(b) Systems security. The government shall notify a common carrier of any interception of wire or electronic communications or any acquisition of call setup information that is to be effected within the premises of such common carrier pursuant to court order or lawful authorization. After notification, such common carrier shall designate an individual or individuals to activate such interception or acquisition forthwith. Such individual(s) shall be available at all times to activate such interceptions or acquisitions. Such interceptions or acquisitions effected within the premises of a common carrier may be activated only by the affirmative intervention of such individual(s) designated by such common carrier.

"(c) Compliance date. To the extent that common carriers providing service within the United States currently cannot fulfil the requirements set forth in subsection (a) of this section, they shall fulfil such requirements within three years from the date of enactment of this Act.

"(d) Cooperation of support service providers and equipment manufacturers. Common carriers shall consult, as necessary, in a timely fashion with appropriate providers of common carrier support services and telecommunications equipment manufacturers for the purpose of identifying any services or equipment, including hardware and software, that may require modification so as to permit compliance with the provisions of this Act. A provider of common carrier support services or a telecommunications equipment manufacturer shall make available to a common carrier on a timely and priority basis at a reasonable and cost-effective charge, any support service or equipment, including hardware and software, which may be required so as to permit compliance with the provisions of this Act.

"(e) Enforcement. The Attorney General shall have authority to enforce the provisions of subsections (a), (b), (c), and (d) of this section. The Attorney General may apply to the appropriate United States District Court for an order restraining or enjoining the provision of service of any common carrier who violates subsection (a), (b), (c), or (d) of this section and for an order mandating the cooperation of a provider of common carrier support services or a telecommunications equipment manufacturer pursuant to the provisions in subsection (d). The District Courts shall have jurisdiction to issue such orders. The Attorney General may also request the Federal Communications Commission to assist in enforcing provisions of this Act.

"(f) Penalties. Any common carrier that violates any provision of subsection (a) of this section shall be subject to a civil penalty of $10,000 per day for each day in violation. The Attorney General may file a civil action in the appropriate United States District Court to collect, and the United States District Courts shall have jurisdiction to impose, such penalties. After consultation with the Attorney General, the Federal Communications Commission may also impose regulatory sanctions or fines otherwise authorized by law.

"(g) Consultation. The Attorney General is encouraged to consult with the Federal Communications Commission and common carrier representatives and to utilize common carrier standards bodies, associations, or other such organizations to discuss details of the requirements, such as those related to capacity, and cost-effective approaches in order to facilitate compliance with the provisions of this Act.

"(h) Funding. The Federal Government shall pay common carriers for reasonable and cost-effective charges directly associated with the modifications required to assure common carrier compliance with the requirements of this Act which are incurred within the three year period set for compliance.

"(i) Definitions. -- As used in this Section --

(1) 'common carrier' means any person or entity engaged as a common carrier for hire, as defined by section 3(h) of the Communications Act of 1934, and includes a commercial mobile service or interconnected service, as defined in section 6002(b) of Public Law 103-66;

(2) 'provider of common carrier support services' means any person or entity who provides services to a common carrier that are integral to processing, directing, forwarding, or completing telephone calls or electronic communication transmissions;

(3) 'wire communication' shall have the same meaning as set forth in subsection 2510(1) of title 18, United States Code;

(4) 'electronic communication' shall have the same meaning as set forth in subsection 2510(12) of title 18, United States Code;

(5) 'intercept' shall have the same meaning as set forth in section 2510(4) of title 18, United States Code, except that with regard to a common carrier's transmission of a communication encrypted by a subscriber, the common carrier shall not be responsible for ensuring the government agency's ability to acquire the plaintext of the communications content, unless the encryption was provided by the common carrier and the common carrier possesses the information necessary to decrypt the communication;

(6) 'concurrent with the transmission of the communication,' as used in section 3(a)(2) of this Act, means contemporaneous with the transmission; but it shall include, with regard to electronic communications, the ability of a government agency to acquire such communications at the conclusion of the transmission, and, with regard to call setup information, the ability to acquire such information either before, during, or immediately after the transmission of the communication;

(7) 'call setup information' shall mean the information generated which identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful

authorization, including information associated with any telecommunication system dialing or calling features or services; and

(8) 'government' means the Government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory or possession of the United States, and any state or political subdivision thereof authorized by law to conduct electronic surveillance."

SEC. 4. COMMUNICATIONS PRIVACY IMPROVEMENT AND MONITORING CLARIFICATION.

Chapter 119 of title 18 is amended by making the following changes:

(1) Cordless telephones.

(a) Definitions. - Section 2510 of title 18, United States Code, is amended

(1) in paragraph (1), by striking ", but such term does not include" and all that follows through "base unit"; and

(2) in paragraph (12), by striking subparagraph (A) and redesignating subparagraphs (B) through (D) as subparagraphs (A) through (C), respectively.

(b) Penalty. - Section 2511 of title 18, United States Code, is amended -

(1) in subsection (4)(b)(i), by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,"; and

(2) in subsection (4)(b)(ii), by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,".

(2) Radio based data communications.

Section 2510(16) of title 18, United States Code, is amended by striking the word "or" at the end of subparagraph (D) and inserting an "or" at the end of subparagraph (E) and adding the following new subparagraph:

"(F) an electronic communication;".

(3) Penalties for monitoring radio communications that are not scrambled, encrypted, or non-public.

Section 2511(4)(b) of title 18, United States Code, is amended by deleting the phrase "or encrypted, then--" and inserting the following:

", encrypted, or transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication, then--".

(4) Technical correction.

Section 2511(2)(a)(i) of title 18, United States Code, is amended by striking out "used in the transmission of wire communication" and inserting in lieu thereof "used in the transmission of a wire or electronic communication".

Section by Section Analysis

SECTION 1. SHORT TITLE

Section 1 provides that the short title of the Act is the "Digital Telephony and Communications Privacy Improvement Act of 1994."

SECTION 2. PURPOSE

Section 2 states the purpose of the Act is to clarify and define the responsibilities of common carriers, providers of common carrier support services, and telecommunications equipment manufacturers to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information (e.g., dialed number information) pursuant to the Federal and state electronic surveillance and pen register and trap and trace statutes. An effective electronic surveillance capability is essential to Federal, state, and local agencies so that they can secure the public safety, effectively enforce the law, and maintain the national security. Without clarification of the increased responsibilities of the telecommunications industry to assist and cooperate, this critical investigative technique will be eroded, if not precluded, by the advances in telecommunications technology.

The statutory requirement for common carriers and others to provide needed assistance to law enforcement agencies in the execution of electronic surveillance court orders and lawful authorizations is a long-standing one. Since 1970, the assistance of common carriers and others has been mandated. In a 1970 amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), Congress enacted a provision specifying that a "communication common carrier [common carrier], landlord, custodian, or other person shall furnish [the government applicant for court-ordered electronic surveillance] forthwith all information, facilities, and technical assistance necessary to accomplish the interception * * *." In return for providing the information, facilities, and technical assistance, the assistance provider is required to be compensated by the applicant for reasonable expenses incurred in providing the assistance. *See* 18 U.S.C. 2518(4).

The foregoing "assistance" provision also has been incorporated in the Foreign Intelligence Surveillance Act of 1978 (FISA) (codified at 50 U.S.C. 1805(b)(2)(B)) and in the pen register/trap and trace provisions of the Electronic Communications Privacy Act of 1986 ("ECPA") (codified at 18 U.S.C. 3134(a), (b)).

The purpose of the legislation is to clarify and define the *nature* and *extent* of this responsibility which arises from the stark mandate of the foregoing laws.

In 1970, the telephone industry was monolithic, and the part of the telecommunications network where government effected electronic surveillance was relatively uncomplicated. since that time, with the breakup of AT&T through divestiture, the,entry of numerous new communications providers in the telecommunications marketplace, and the introduction of many new (and often proprietary) technologies, services, and features, the telecommunications networks have become more varied, advanced, and complicated. Though unintended, the complexities of the telecommunications networks create, and will continue to create, impediments to Federal, state, and local government agencies as they attempt to execute electronic surveillance and pen register and trap and trace court orders and authorizations.

With the passage of the ECPA amendments to Title III, electronic communications have received statutory privacy protection as well, and the term common carrier has been replaced with the broader terminology of provider of wire or electronic communication service. However, intercepting voice communications and acquiring the attendant dialing information remain of the greatest importance to government agencies; and the principal area where technological impediments have been encountered is within the networks of wireline and cellular common carriers.

Solutions have not always been readily available for existing problems, and they may not be for the future problems that are foreseen in the emerging technologies, services, and features. Such solutions also take time and may require significant "capital" outlays. As a result, industry and government agencies have been uncertain as to the nature and extent of the foregoing "assistance" provision. In particular, key questions exist in terms of who is responsible for efforts to remove the impediments; how quickly the impediments should be removed; what the consequences are, if any, for not removing them in a timely fashion; and who is responsible for paying the costs.

Because of concerns about compromising investigations, harming law enforcement and common carrier relationships, and due to the prospect of substantial delays, government agencies have been reluctant to pursue contempt or other legal remedies to resolve this issue. Also, because of the variety of technological impediments and the differences in levels of effort required to remove them, the government has been concerned that a particular judicial ruling may have only limited precedential value. Consequently, as things now stand, common carriers and other communications service providers ultimately decide what they will do to remove technological impediments, and when. When carriers and providers have acted, it frequently has taken months, and in some instances years, for ad hoc technical solutions to be developed, and the rate and breadth of their deployment have been uncertain. Thus, since the mid-1980's, technological impediments have frustrated, in whole or in part, the execution of a number of court orders for electronic surveillance, pen registers, or trap and traces, while the means of approaching and resolving the overall problem of the negative impacts of advanced telecommunications technology on electronic surveillance has eluded government and industry.

It has been observed that while it may be somewhat difficult and expensive to remove some existing impediments forthwith, that where new, advanced services and features are still under development or where upgrades are being prepared that technological solutions could be applied with significantly less difficulty and expense. Additionally, some common carriers, especially those who only more recently have entered the marketplace, have noted that they are not familiar with all of the electronic surveillance requirements of government agencies. Finally, some common carriers have stated that they rely on certain support service providers and equipment manufacturers to provide telecommunications service, and that without the help of those entities they may be unable to make the modifications required to remove the impediments and meek the requirements of government agencies.

Although Government and industry have made efforts to resolve this problem, after several years of discussion and consultation, the basic concerns and issues remain: what are the requirements of government agencies in this area; who is responsible for removing the impediments that impact on these requirements; how quickly must these requirements be met; what are the consequences, if any, for not meeting them on a timely basis; and who is responsible for paying the costs. This legislation addresses and resolves these concerns and issues.

The "Purpose" section also indicates that, excepting section 4, the legislation is not intended to alter any provision in the Federal electronic surveillance, pen register, or trap and trace statutes, or those of any state or other jurisdiction, such as those regarding the authority to intercept communications or install or use pen register and trap and trace devices; the current duty to provide assistance and receive payment therefore; causes of action; civil liability; or good faith defenses. The underlying purpose of the legislation is to clarify and define the responsibilities of common carriers such that government agencies can *maintain* their ability to properly and effectively execute electronic surveillance-related court orders and lawful authorizations.

An additional purpose to the Act, as set forth in section 4, is to improve communications privacy protection for users of cordless telephones, certain radio-based data communications and networks, communications transmitted using certain privacy-enhancing modulation techniques, and to clarify the lawfulness of quality control and service provision monitoring of electronic communications.

SECTION 3. NEW SECTION

Chapter 109 of title 18, U.S.C. is amended by adding a new section, section 2237, entitled: "Common carrier assistance to government agencies." Amendment of this chapter is made in order to avoid having to amend three separate, yet interrelated, Federal statutory regimes: Title III (18 U.S.C. 2510 *et seq.*); FISA (50 U.S.C. 1801 *et seq.*); and the pen register and trap and trace provisions of the ECPA (18 U.S.C. 3121 *et seq.*).

Common carrier assistance: assistance requirements

Section 3(a) sets forth the requirements of government agencies when conducting electronic surveillance and pen register and trap and trace investigations. These requirements, which are generic in nature, were developed by the FBI and include input from representatives of various Federal, state, and local law enforcement agencies that utilize electronic surveillance extensively. These requirements relate to the capabilities needed to accomplish effectively the interception of communications and the acquisition of call setup information. The Government intentionally has eschewed setting any technical standards because it does not desire to "dictate" particular technological solutions. Further, owing to the diversity (and often proprietary nature) of each carrier's network and the variations in approaches that can be taken to achieve compliance, it is the Government's position that each common carrier is best positioned and qualified to determine how it will meet the requirements in the most cost-effective way.

Although the requirements set forth in section 3(a) constitute the first legislative listing of the government's requirements, the FBI states that for many years most, if not all, of these requirements have been known to the security offices of the major local exchange carriers, interexchange carriers, and cellular carriers. (Security offices, usually are designated by common carriers to receive service of the court orders and authorizations and to provide law enforcement agencies with the information and assistance required to execute the court orders and authorizations.)

The legislation requires common carriers to provide "forthwith" the capability and capacity necessary to permit the government to conduct electronic surveillance, pen register, and trap and trace investigations effectively. The requirement of providing assistance "forthwith" is not new. It is found in the current language of 18 U.S.C. 2518(4), 3124, and 50 U.S.C. 1805(b)(2)(B). The language concerning capability and capacity is included to underscore the need for a common carrier to afford not only an ability to effect the interception of communications and the acquisition of call setup information (which includes dialed number information) but also the ability to accommodate without delay all court orders and authorizations for electronic surveillance, pen registers, and trap and traces that may be served on such common carrier by the various Federal, state, and local government agencies.

Within section 3(a)(1), it is stated that the foregoing, capability and capacity must accommodate the "expeditious" and "simultaneous" execution of all court orders and authorizations. Frequently, it is essential to implement the interception of communications or acquire dialed number information expeditiously in order to obtain information critical to saving lives, making arrests, and seizing evidence and contraband, such as drugs, illegal weapons, bombs and other explosive devices.

The capability and capacity requirement is also very important inasmuch as a number of government agencies must be able to execute a number of court orders and authorizations simultaneously. The FBI states that over the past decade a number of court orders and authorizations were not fully executed, or were not even sought, because of certain technological impediments and capacity shortfalls, such as insufficient "port" capacity in the cellular mobile switching offices (MSO's). At any particular time a number of Federal, state, and local government agencies may be competing to execute electronic surveillance and pen register court orders regarding certain telecommunication facilities, the access point for which is of limited capacity. Inasmuch as communications interceptions and dialed number acquisitions increasingly will be activated from within common carrier premises, including switching offices, it is critical that there be sufficient capacity to accommodate completely the concomitant needs of all government agencies.

As discussed below with regard to section 3(g), since common carriers' technological responses to the requirements will vary by common carrier and by the technology being addressed, and because historically each carrier has been subject to varied numeric demands in terms of court orders or authorizations, the Government intends to consult with common carriers and telecommunications industry representatives in a number of areas, such as in the area of capacity, in order to assist in facilitating proper sizing approaches and cost-effective compliance. Further, it is expected that most common carriers can ensure compliance in the future and gauge the future demands of government agencies by reviewing their records as to the numbers of, and trends in, current and past court orders and authorizations and extrapolating therefrom the sizing required to meet future demands. Finally, the increasing availability of "modular" and incremental technical approaches will allow common carriers to respond flexibly throughout their networks to the demands of government agencies in a cost-effective manner.

Section 3(a)(2) specifies that common carrier networks must afford government agencies an ability to intercept communications and acquire call setup information "concurrent" with the transmission of the communication to or from the subscriber's facility or service that is the subject of the court order or authorization, to the exclusion of communications or information concerning any other subscriber, and without regard to the mobile nature of the subject subscriber's facility or service or the use by that subscriber of any custom features or services offered by the common carrier.

It is important that government agencies can intercept communications concurrent with the transmission of the original communication. Further, the associated requirement of being able to acquire call setup information concurrent with the subject transmission also is essential. For example, it is critical for government agencies to be able to intercept communications as they occur so they can respond immediately to life-threatening circumstances and react promptly and effectively to criminal activity in terms of making needed arrests, seizing evidence, and interdicting contraband, such as drugs, illegal weapons, bombs and other explosive devices.

The separation of signaling transmission paths from communications paths also can impede government agencies who must be able to associate the intercepted communication with the calling or called party. Aside from the negative evidentiary impact caused, this circumstance can hamper government agencies in their efforts to effectively "minimize" the monitoring and recording of non-criminal communications. Consequently, there is a requirement that common carriers can assure that call setup information will be available "concurrent with the transmission of the communication" that is the subject of the court order or authorization.

Owing to the varying availability of contemporaneous call setup information, the definition of "concurrent with the transmission of the communication" found in section 3(i)(6) specifies that the "concurrence" requirement is satisfied if such information can be acquired by government agencies either before, during, or immediately after the transmission of the communication. It is the clear preference of government agencies that common carriers will attempt to afford the ability to acquire this information before the transmission of the communication whenever reasonably feasible. Similarly, because of the difficulty of intercepting certain "electronic communications" concurrent with their transmission, the foregoing definition states that providing government agencies an ability to intercept such information at the conclusion of the transmission will satisfy the requirement.

The requirement that government agencies will have the ability to isolate the communications and call set up information of the subjects of electronic surveillance to the exclusion of the communications and call setup information of other subscribers is a basic and a long-standing one. Government agencies do not want to be faced with the prospect of having to "sort through" a tangle of communications which include those of innocent individuals who have the misfortune of having their communications "bundled" or otherwise commingled with those of the interception subject in the telecommunication transmission process. This requirement is being challenged by the increased use of digital transport, multiplexing, and fiber optics closer to the premises of the interception subject. Hence, common carriers must assure that there are means to access and isolate communications and call setup information, yet in a fashion that does not compromise the interception or acquisition effort.

The increasingly mobile nature of telecommunications facilities and service also has created impediments to the effective execution of electronic surveillance. With today's cellular telephony, communications can be "handed off" within and between networks and can be routed about such that they bypass interception access points, even when they are established within the premises of a cellular common carrier. It is believed that the communication interception and call setup information acquisition requirements of government agencies can be met by common carriers affording mobile service by drawing upon existing technologies and programming and routing capabilities and by coordinating efforts with other mobile carriers. This same requirement also has application to other mobile features and services which permit subscribers to program or otherwise direct communications to any facility designated by the subscriber (e.g., "follow me service"), as well as to the emerging mobile services encompassed in personal communications services (PCS) and other radio frequency-based mobile communications services.

Section 3(a)(2) specifies that the communication interception and call setup information acquisition requirement includes an ability to obtain such communications and information notwithstanding the use by the subject subscriber of any telecommunications custom "features" offered by the common carrier. The most notable feature impediment to effective electronic surveillance is "call forwarding." This feature permits a subscriber, whose telecommunications facility (and telephone number) is the subject of a court order or authorization, to redirect in-coming calls from that facility to other facilities. Such call redirection can be accomplished according to established programs or even randomly and dynamically. In the past, government agencies frequently have proceeded by securing additional court orders for those new facilities to which the calls have been "forwarded" or redirected by the subject subscriber of the court order or authorization. This circumstance has resulted in government agencies having to obtain more court orders or authorizations than typically would have been required; in criminal communications escaping timely interception; and, in some instances, in additional households unnecessarily becoming targets of electronic surveillance.

Section 3(a)(3) includes the requirement that there be an ability to intercept the content of communications and acquire call setup information unobtrusively and with a minimum of interference with any subscriber's telecommunications service. This language mirrors language currently found in 18 U.S.C. 2518(4), 3124, and 50 U.S.C. 1805(b)(2)(B), and it is intended to prevent subjects of electronic surveillance and pen register and trap and, trace investigations and others from detecting the surveillance effort.

Section 3(a)(4) contains the requirement that, once intercepted or acquired, the government agency would be able to receive the communication or call setup information in a generally available format at a location identified by the government agency distant from the subject's facility, from the interception or acquisition access point, and from the premises of the common carrier. This requirement is not new and is intended to maintain the current ability of government agencies to monitor, record, minimize, and otherwise properly administrate electronic surveillance and pen register and trap and trace investigations. This requirement is fundamentally important, since without it the safety of law enforcement officers and government employees would be put at risk, the interception or acquisition effort easily could be compromised through detection, and the effective execution of the surveillance search would be significantly disrupted.

Currently, once access has been obtained within the local loop or the common carrier's central office facilities, the communications and call setup information are transmitted back to the law enforcement agency's facility or monitoring plant, usually within the agency's office. The transmission most frequently occurs via line facilities provided by the common carrier.

The language which states that the communications and call setup information are to be received in a generally available format is intended to bake clear that government agencies do not expect common carriers to translate digital transmissions to analog, etc. before affording transmission to them. Rather, it is expected that a common carrier would utilize a transmission format that was consistent with that of the communication being intercepted or acquired at the time of access, such as analog voice channel on a local loop, D4 formatted T–1 circuit, ISDN Primary Rate Interface circuit, etc. On the other hand, government agencies understand that they, not the common carriers, are responsible for processing the communications intercepted and the call setup information acquired.

Section 3(a)(4) also indicates that in some emergency or exigent circumstances that a government agency by necessity may have to access and monitor communications or dialed number information on the common carrier's premises. Government agencies understand that common carriers are not desirous of having government personnel carry out all aspects of a surveillance on common carrier premises, and it is understood that the government's presence in common carrier premises should only occur in emergency or exigent circumstances. Also, government agencies are not expecting common carrier personnel to assist in the monitoring aspects of executing a court order or authorization.

Section 3(b) specifies that government agencies shall notify common carriers of any wire or electronic interceptions or any call setup acquisitions that are to be effected within the premises of such common carrier pursuant to court order or authorization. Common carriers are required to designate individuals to activate such interceptions or acquisitions. These individuals are required to be available at all times to activate the interceptions or acquisitions. The requirement can be met by such individuals being "on call," in order to promptly respond to governmental needs as necessary. The requirement does not mean that the designated individuals actually must be on the premises at all times or that 24 hour-a-day work shifts must be established. Such interceptions or acquisitions may be activated only by the affirmative intervention of such individuals.

This provision recognizes that the access point for intercepting communications and acquiring call setup information increasingly will originate within common carrier premises. Such premises include buildings, switching offices and facilities, and network elements (e.g., signaling transfer points) maintained by the common carriers. Since it is important that these facilities, as well as the entire telecommunications network, remain secure, it is a requirement that all such access be initiated directly only by individuals designated by the common carrier.

Government agencies are not seeking the authority or ability to remotely activate interceptions within the premises of a common carrier in a fashion that bypasses personnel designated by common carrier. All executions of court orders or authorizations which require access to the switching facilities or other premises will be made through the individuals authorized and designated by the common carrier. Activation of interceptions or acquisitions originating in local loop wiring or cabling can be effected by government personnel or by individuals designated by the common carrier, depending upon the amount of assistance the government requires.

Section 3(c) states that to the extent common carriers providing service within the United States currently cannot fulfill the requirements set forth in subsection (a), they shall fulfill such requirements within three years from the date of enactment of the Act. This section makes clear that the focus of compliance is on common carriers within whose networks most of the electronic surveillance occurs.

Nearly all wireline and wireless voice communications are provided by local exchange carriers, interexchange carriers (and increasingly by service "resellers" and competitive access providers (CAPS)), and by cellular carriers (and soon by providers of Personal Communications Services (PCS) and satellite based mobile communications providers). These entities are common carriers, and historically they have been subject to regulation. Since most electronic surveillance is effected within the networks of common carriers, the coverage has been scaled to focus only on those service providers within whose networks the core technological problems exist.

Although certain categories of electronic communication service providers (e.g., PBX and computer network operators) who currently have assistance responsibilities under Federal and state laws are excluded from the provisions of this legislation, nevertheless it is expected that such providers will continue to fulfill their statutory responsibilities and undertake voluntarily to accommodate the electronic surveillance needs of government. If significant technological impediments arise within their networks in the future due to inattention to government requirements or due to inaction in addressing them, consideration would have to be given to seeking expansion in the coverage of the instant legislation to include such entities.

The language of the section is also intended to indicate that common carriers still must fulfill their assistance responsibilities under 18 U.S.C. 2518(4), 3124, and 50 U.S.C. 1805(b)(2)(B) by furnishing requested information, facilities, and technical assistance, to the extent possible, during the three year grace period set for compliance. There should be no relaxation in common carrier efforts to assist government agencies in effectively executing court orders and authorizations.

Some common carriers, such as "resellers" and competitive access providers (CAPS), either may not own any equipment or facilities or the equipment or facilities they own may be such that they are not capable of effecting interceptions or acquisitions under this Act. In such cases, it is expected that such service entities would rely on the compliance of the common carrier whose facilities they lease, etc., and that they likely would seek from such common carrier legal assurances that compliance will be achieved within the statutory compliance period or that such common carrier would indemnify them for any liability or penalty they bay incur if compliance is not met. If a common carrier leases a portion of its switching or other network facilities to an end user and such facilities are not under the carrier's control, then the carrier shall not be obligated to make that portion compliant as long as it remains beyond the common carrier's control.

The date for common carrier compliance is set at within three years from the date of enactment of the Act. The Government believes that this is a reasonable period within which the needed technological solutions can be identified, tested, and deployed within the networks of common carriers. As discussed below, common carriers receive important assistance and cooperation of equipment manufacturers and common carrier support service providers so that timely compliance can be achieved.

The coverage of compliance includes needed modifications to existing systems and networks. (embedded base) as well as to future systems and networks (those—fielded, after the three year compliance period).

Section 3(d) provides that common carriers shall consult in a timely fashion with providers of common carrier support services and telecommunications equipment manufacturers so that any needed modifications to services and equipment, including hardware and software, can be made, and thus help to ensure common carrier compliance within three years. This section further specifies that a provider of common carrier support services and a telecommunications equipment manufacturer shall make available to a common carrier on a timely and priority basis, at a reasonable and cost-effective charge, any support services or equipment required so as to permit compliance with the provisions of the Act. The responsibilities of common carrier support service providers and equipment manufacturers are added to the legislation to indicate that they have an important role in ensuring that court orders and authorizations are not frustrated.

Assistance and cooperation from support service providers and equipment manufacturers are increasingly important, as services and equipment become more sophisticated and as common carriers rely on "outside" companies to provide them with these components. Although the direct burden of compliance falls on common carriers, nevertheless statutory responsibilities are conferred upon these support service providers and equipment manufacturers without whose help the common carriers likely could not comply. One of the major objections to the compliance date and attendant penalty provisions raised in the past by representatives of the Regional Bell operating Companies (RBOC's) was the concern that local exchange carriers must rely on equipment manufacturers and others in order to meet many of the requirements.

Under provisions of the Modified Final Judgment (MFJ) of the consent decree regarding the Government's antitrust case against AT&T, local exchange carriers are precluded from engaging in telecommunications equipment manufacturing. However, a Department of Justice memorandum concludes that Judge Greene's order would not be an impediment to a common carrier's effecting limited, noncommercial modifications to network facilities, services, or equipment, the sole purpose of which would be to prevent the frustration of statutorily-based court orders and authorizations designed to ensure effective law enforcement, the public safety, and the national security.

Section 3(e) states that the Attorney General of the United States shall have the authority to enforce the provisions of subsections (a), (b), (c), and (d) of section 3. In order to, avoid disparate enforcement actions throughout the country in ways that could be burdensome for common carriers, the responsibility for enforcing these provisions is vested in the Attorney General of the United States through the Department of Justice and the Offices of the various United States Attorneys.

In particular, the Attorney General is specifically given the authority to apply to an appropriate United States District Court for an order restraining or enjoining the provision of service by any common carrier who violates the foregoing subsections of section 3. Similarly, to ensure common carrier compliance, the Attorney General may apply for an order, such as a writ of mandamus, which mandates the cooperation of a provider of common carrier support services or a telecommunications equipment manufacturer pursuant to the provisions in subsection (d). The intent is that there be no excuse offered by common carriers that they cannot comply because of unresponsiveness on the part of such support service providers and equipment manufacturers. The Federal district courts are specifically given jurisdiction to issue such orders. Additionally, the Attorney General may request the Federal Communications Commission. (FCC) to assist in enforcing provisions of the Act. This provision recognizes the wide-ranging authority of the FCC over common carriers and others in the telecommunications industry.

Section 3(f) specifies that any common carrier that violates section 3(a) shall be subject to a civil penalty of $10,000 per day for each day in violation. The Attorney General is authorized to file a civil action to collect, and the Federal district courts have jurisdiction to impose, such fines. The FCC may also impose regulatory sanctions or fines authorized by law.

Section 3(g) provides that the Attorney General is encouraged to consult with the FCC and common carrier representatives and to utilize common carrier standards bodies, associations, and other such organizations to discuss details of the requirements, such as those related to capacity, in order to facilitate compliance with the provisions of the Act. This subsection evidences an intention on the part of Government to help common carriers achieve compliance with as little difficulty as possible, and it the most cost-effective way possible. Through detailed discussions, narrow and technical questions from common carriers can be answered and other concerns addressed.

Such fora also may act as potential clearinghouses for promising, cost-effective technological approaches and solutions, which would likely reduce costly and duplicative independent efforts on the part of each common carrier. The FBI and other law enforcement agencies have been meeting with industry (largely common carrier) technical committees for nearly two year's in this regard, currently under the auspices of the Alliance for Telecommunications Industry Solutions' Electronic Communications Service Provider Committee (ECSPC). However, because of the voluntary basis and elective nature of participation in and commitment to this body, its lack of authority to require the implementation of solutions or to assign funding responsibility, and given that there is no clear legal mandate to fulfill government's requirements on a timely basis, these committees have not been effective to date in engendering the development, let alone the implementation, of the required solutions. With legislation mandating future compliance and addressing funding concerns, it is reasonable to assume that common carriers and others will utilize such committees in a more meaningful and beneficial fashion.

Section 3(h) states that the Federal Government shall pay common carriers for reasonable and cost-effective charges directly associated with the modifications required to assure common carrier compliance with the requirements of this Act which are incurred within the three year period set for compliance.

The Federal Government has concluded that it should compensate common carriers for reasonable and cost-effective charges associated with devising and implementing the modifications required which remove the technological impediments and assure common carrier compliance with the government's requirements established in section 3(a). The remuneration covers charges incurred within the three year period set for compliance with regard to certain interim solutions to remove the impediments that most concern the Government; for the cost of modifying existing networks, services, facilities, and features; and for research and development and testing efforts associated with making future networks, services, and features compliant with the government's requirements. Once solutions have been identified, it is expected that they would be incorporated into successive generations of service and, where feasible, into new services without additional charge to the Government.

Section 3(i) sets forth definitions for sections 1–3 of the Act. The term "common carrier" means any person or entity engaged as a common carrier for hire, as defined by section 3(h) of the communications Act of 1934, and includes a commercial mobile service or interconnected service, as defined in section 6002(b) of Public Law 103–66. This definition encompasses such service providers as local exchange carriers, interexchange carriers, service "resellers," competitive access providers (CAPS), cellular carriers, personal communications services (PCS), satellite-based service providers, and any other common carrier who offers wireline or wireless service to the general public.

The term "provider of common carrier support services" meansany person or entity who provides services to a common carrier that are integral to processing, directing, forwarding or completing telephone calls or electronic communication transmissions. There are currently over one hundred such support service providers that provide common carriers with specialized support services.

The terms "wire communication" an "electronic communication" have the same meanings as set forth at 18 U.S.C. 2510(12) and 2510(12), respectively, under Title III, as amended by the ECPA.

The term "intercept" has the same meaning as set forth at 18 U.S.C. 2510(4), except that with regard to a common carrier's transmission of a communication encrypted by a subscriber, the common carrier shall not be responsible for ensuring the government agency's ability to acquire the plaintext of the communications content, unless the encryption was provided by the common carrier and the common carrier possesses the information necessary to decrypt the communication. The term "intercepts" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication * * *." The term "contents" includes "any information concerning the substance, purport, or meaning of [a] * * * communication." 18 U.S.C. 2510(8). The language in the definition of "intercept," as used in this legislation, is intended to clarify that a common carrier has no obligation to decrypt communications that have been encrypted by the subscriber, such that the conversation or data transmission can immediately be understood by the government, unless the encryption was provided by the common carrier and the carrier possesses the information necessary to decrypt the communication.

The term "concurrent with the transmission of the communication" means contemporaneous with the transmission of the communication, but it also includes, with regard to electronic communications, the ability of the government to acquire such communications at the conclusion of the transmission, and, with regard to call setup information, the ability to acquire such information either before, during, or immediately after the transmission of the communication.

The definition of "concurrent with the transmission of the communication" found in section 3(i)(6), is somewhat broader than term might imply on its face. The definition was broadened due to the varying feasibility of effectively intercepting electronic communications contemporaneously and the varying availability of call setup information contemporaneous with the transmission of the communication with which it is associated. Because of the difficulty of intercepting certain electronic communications concurrent with their transmission, the foregoing definition states that providing an ability for government agencies to intercept such information at the conclusion of the transmission will satisfy the requirement. The definition also specifies, with regard to call setup information that the "concurrence" requirement is satisfied if such information can be acquired by government agencies either before, during, or immediately after the transmission of the communication. It is the clear preference of government agencies that common carriers will attempt to assure an ability to acquire this information before the transmission of the communication whenever reasonably feasible.

The term "call setup information" means the information generated which identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization, including information associated with any telecommunications system dialing or calling features or services. For voice communications, this information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted, or caused to be transmitted. In pen register investigations, these are the pulses, tones, or messages which identify the numbers dialed from the facility that is the subject of the court order or authorization. In trap and trace investigations, these are the incoming pulses, tones, or messages which identify the originating number of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order or authorization.

With regard to electronic communications, the information is that generated during the establishment of communications or the transmission of a protocol data unit, such as a datagram, that identifies the origin and destination of the communication. For data services, this information is typically the source (calling) address and destination (called) address contained in fields of the data unit, such as the header of a frame or packet.

The call setup information also encompasses numbers identified incidental to calls where calling features or services are used.

The term "government" means the Government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any state or political subdivision thereof authorized by law to conduct electronic surveillance.

SECTION 4. COMMUNICATIONS PRIVACY IMPROVEMENT AND MONITORING CLARIFICATION

Section 4 includes several amendments to Chapter 119, United States Code, which includes Title III, with regard to communications privacy improvements and clarifications concerning monitoring of electronic communications.

In section 4, amendments are made to the definitions found in 18 U.S.C. 2510(1) and (12). The purpose of the amending language is to provide communications privacy protection to cordless telephone communication transmissions occurring in the radio link between the telephone handset and base station.

Because of the ease with which communications occurring in the radio portion of cordless telephone transmissions could be overheard through the use of commercial radio receivers, scanners, and similar cordless telephones operating in the same area, Congress chose not to confer statutory privacy protection upon the radio portion of cordless telephone communications or to criminalize the interception of same in the 1986 ECPA amendments to Title III. However, since then, advances in cordless telephony have resulted in the mass-marketing of various types of cordless telephones, many of which are considerably more difficult to intercept than the earlier models. Because newer versions and types of cordless telephones incorporate features and technology that typically afford greater security to the user, there now exists a basis for providing full statutory privacy protection to cordless telephones. Even absent the prior statutory privacy protection, the view that certain cordless telephone users nonetheless retain Fourth Amendment privacy protection under the "reasonable expectation of privacy" criteria has been asserted. *See United States* v. *Smith*, 978 F.2d 171, 176 (5th Cir. 1992). This amendment now confers the same communications privacy protection for the millions of cordless telephone users as is currently afforded to cellular telephone users.

The penalty provisions for intercepting cordless telephones are also made consistent with those for intercepting cellular telephones, by the amendments to 18 U.S.C. 2511(4)(b)(i) and (ii) set forth in this section.

Section 4 also includes language which amends 18 U.S.C. 2510(16), communications deemed to be "readily accessible to the general public" with regard to radio communications, and the exceptions thereto. The excepted categories currently covered under section 2510(16)(A)–(E) enjoy privacy protection because they usually are not susceptible to interception by the general public. Added to these categories is the new category of "electronic communication." The intention is to provide clarification that there is protection for all forms of electronic communication, including data, even when they may be transmitted by radio.

Section 4 also amends the penalty provisions set forth in 18 U.S.C. 2511(4)(b) by adding language that specifies a similar penalty for intercepting communications "transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication." The purpose of the amendment is to treat communications using such modulation techniques in the same fashion as those where encryption has been employed to secure communications privacy.

Finally, section 4 amends 18 U.S.C. 2511(2)(a)(i) by clarifying that it is not unlawful for a switchboard operator, officer, employee, or agent of a wire or electronic communication service to intercept, disclose, or use an "electronic communication," in the same fashion as a wire communication, in the normal course of his employment while engaged in any activity which is necessary incident to the rendition of his service or to the protection of the rights or property of the provider of the service. This technical correction is designed to put the handling of electronic and wire communications on the same footing.

LAW ENFORCEMENT REQUIREMENTS FOR THE SURVEILLANCE OF ELECTRONIC COMMUNICATIONS

INTRODUCTION

In July 1992, the Federal Bureau of Investigation, in cooperation with federal, state, and local law enforcement agencies, published a document entitled Law Enforcement Requirements for the Surveillance of Electronic Communications. The document outlined law enforcement's nine requirements for the surveillance of electronic communications. As a result of discussions between law enforcement and industry, law enforcement has prepared clarifications and examples to support the requirements contained in the July 1992 document. These clarifications and examples respond to specific questions raised by the electronic communications industry. This document states law enforcement's nine requirements and provides supporting clarifications and examples, thereby superseding the July 1992 document.

BACKGROUND

The primary mission of federal, state, and local law enforcement agencies is to enforce the laws of their respective jurisdictions. Various federal and state laws authorize the interception of electronic communications for the investigation of serious crimes. This extraordinary technique is critical to law enforcement's mission. Law enforcement agencies can conduct lawfully authorized electronic surveillance when traditional investigative techniques are determined to be ineffective or too dangerous.

To conduct lawful electronic surveillance, law enforcement agencies require access to the communications associated with the subject of investigation (that is, intercept subject). In this process, law enforcement agencies rely on the cooperation and assistance of the providers of electronic communications services. A number of legal instruments permit law enforcement to collect information on or about a subject's electronic communications. These instruments include court orders (such as pen register, Title III, traps, and traces), search warrants, subpoenas, and other lawful authorizations.

Recent and continuing advances in electronic communications technology and services challenge, and at times erode, the ability of law enforcement agencies to fully implement lawful orders to intercept communications. These advances also challenge the ability of electronic communications service providers to meet their assistance responsibilities. The law enforcement community needs the continued cooperation of electronic communications service providers to meet the challenges of conducting electronic surveillance on emerging and future technologies. Law enforcement is not seeking to slow the pace of the evolution of electronic communications. In fact, advanced communications features and services benefit law enforcement and the American public. As new technologies and services emerge, law enforcement is attempting only to ensure that capabilities exist for protecting public safety through the use of lawful interception.

SCOPE

This document presents the requirements of federal, state, and local law enforcement agencies to conduct lawful electronic surveillance with regard to users of electronic communications services. Its purpose is (1) to serve as a framework for continued cooperation with the electronic communications industry in the development of approaches for meeting law enforcement's electronic surveillance requirements, and (2) to preserve electronic surveillance capabilities associated with intercept authority as established by applicable federal and state laws.

The requirements are intended to set out key elements needed for the technical and operational implementation of lawful interceptions of electronic communications. Although the requirements are intended to be broad enough to address existing or future communications technologies, the clarifications and examples supporting the requirements may be specific to a current technology or service. As additional technologies emerge, new communications services and features will be introduced after the publication of this document. Consequently, the information presented in this document may not be all-inclusive. Law enforcement recognizes the need to ensure an understanding of the requirements as the electronic communications industry accommodates the requirements in the development of technologies and services. Law enforcement also understands the need to periodically clarify the information presented in this document to account for new services and features identified by service providers.

Access to the communications of an intercept subject is made available by the service provider in accordance with a lawful authorization from law enforcement. As is the case under current statute, "No cause of action shall lie in any court against any provider of wire or electronic communications service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter."[1] Law enforcement's requirements in no way alter the provisions of existing statutes.

DOCUMENT ORGANIZATION AND MAINTENANCE

The remainder of this document is organized into two sections followed by a glossary. Section 2 presents law enforcement's nine requirements for the surveillance of electronic communications. These nine requirements are listed in bold type and are the same as those presented in *Law Enforcement Requirements for the Surveillance of Electronic Communications,* July 1992. The words used to express Requirements 1, 3, and 5 have been modified to better convey their intent based on comments received from industry. The textual modifications are as follows:

- In Requirement 1, the original text was modified to clarify that the requirement is for access to communications transmitted to and from any identifier associated with the intercept subject (not just the identifier of the intercept subject's terminal equipment). Text was also added to clearly convey that a service provider served with a lawful authorization is responsible for providing law enforcement with access to an intercept subject's communications while the subject is within service areas operated by that service provider. Access is required as long as the service provider maintains access to the intercept subject's communications. Law enforcement is not asking for an automatic, seamless, nationwide intercept capability for subjects traveling across multiple service provider boundaries. *In all circumstances, access to network features used to intercept a subject's communications is controlled by service providers and not by law enforcement agencies.*
- In Requirement 3, the term "remote" and the words "away from the intercept access point and/or the intercept subject's terminal equipment" have been deleted to remove confusion regarding the intent of this requirement. The changes reinforce the intent of the requirement. Once a service provider has access to the intercepted communications, law enforcement requires delivery of the communications to a designated monitoring facility. Again, access to any intercept feature is controlled by the service provider and not by law enforcement agencies.
- In Requirement 5, the words "prior to intercept implementation and during the intercept" were moved to the end of the sentence to clarify the requirement. Requirement 5 states that information is required to verify the association of the intercepted communications with the intercept subject. This requirement also states that information on a subject's services and features is required and may be requested before intercept implementation or during the intercept.

Section 3 provides a set of supporting clarifications and examples for each requirement. A glossary containing a list of key words and phrases used in the requirements follows Section 3.

Due to the continuing evolution of electronic communications technology, this document will be reviewed periodically and updated as needed. Any comments or recommendations should be forwarded to:

Assistant Director,
Information Resources Division,
Federal Bureau of Investigation,
JEH FBI Building,
Washington, DC

* * * * *

Requirement 6. Law enforcement agencies require service providers to make provisions for implementing a number of simultaneous intercepts. (Intercept demand will be estimated through a cooperative industry and law enforcement effort.)

---

[1] 18, U.S.C. 2511(2)(c)(ii)

Requirement 7. Law enforcement agencies require service providers to expeditiously provide access to the communications of the intercept subject.

Requirement 8. Over the intercept period, law enforcement agencies require that the reliability of the services supporting the intercept at least equals the reliability of the communication services provided to the intercept subject.

Requirement 9. Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the service providers.

CLARIFICATIONS AND EXAMPLES

The nine requirements presented in Section 2 are restated in this section in bold type. Paragraphs containing clarifications and examples follow each requirement as a means for conveying overall intent. Law enforcement's surveillance authorities include all forms of electronic communications. However, as a result of intensive discussions with the telecommunications industry, most of the clarifications and examples in this section are in terms of telephony, but apply equally to all electronic communications service providers. The clarifications are only illustrative and are an aid for interpreting the intention of requirement. The nine requirements in bold type fully encompass and reflect law enforcement's requirements for lawful intercepts and are not intended to be replaced or limited by the clarifications and examples provided in this section.

REQUIREMENT 1 (COMMUNICATIONS ACCESS)

Law enforcement agencies require access to the electronic communications transmitted, or caused to be transmitted, to and from the number, terminal equipment, or other identifier associated with the intercept subject throughout the service areas operated by the service provider served with a lawful authorization. Law enforcement agencies also require access to generated call setup information necessary to identify the calling and called parties. Law enforcement agencies will coordinate delivery of these communications with the service provider in accordance with Requirement 3 for each service area.

The primary requirement of law enforcement agencies is for access to the electronic communications transmitted, or caused to be transmitted, to and from the intercept subject. In all circumstances, access to network features used to intercept a subject's communications is controlled by service providers and not by law enforcement agencies. The requirement for access to an intercept subject's communications by law enforcement does not imply automatic activation or deactivation of intercepts. Law enforcement agencies will continue to interface with service provider security personnel to request intercept activation and deactivation.

Under Requirement 1, access to an intercept subject's communications includes call setup information and call content. Law enforcement agencies need access to call setup information (for example, originating line/number identification, terminating line/number identification) for all completed and attempted calls. An attempted call is a call that was initiated, but failed to establish a connection between the calling and called parties (for example, when a busy signal was received). Access to call content is required for calls placed by and to the intercept subject, including calls that have been redirected or have multiple call recipients. The obligation of service providers to provide access when custom calling features are invoked depends on whether the service provider that received the authorized intercept request maintains access to the call.

The requirement for lawful access to call content and call setup information also applies to mobile telecommunications services. Law enforcement requires access to an intercept subject's communications throughout the service areas operated by the service provider served with a lawful authorization. With the use of emerging technologies, the location of an intercept subject's access to the network may vary during a call or call attempt (for example, while roaming or when redirecting calls). Law enforcement recognizes the need to coordinate the delivery of communications with service providers before interception occurs.

CALL SETUP INFORMATION

Law enforcement agencies require access to all available call setup information for all attempted and completed calls originated by or terminating to the intercept subject. Call setup information includes, but is not limited to the following:

- Information regarding the intercept subject's line[2]
- Information regarding the calling party's line
- Dialing and signaling information generated by the intercept subject
- Directory numbers used in transferring or forwarding calls
- Notification that a call or call attempt occurred.

Line Information for Terminating Calls. Law enforcement agencies require access to call setup information for all completed and attempted calls to the intercept subject. In this case, call setup information refers to information on both the subject's and the calling party's line. Access to information about the subject's line is required for all calls terminating to the intercept subject. Access to information about the calling party's line is required when it is delivered to the service provider supporting the called intercept subject's communications. The type of line information available for both parties depends on the communications services in use by the calling party and the intercept subject. Exhibit 3–1 lists a number of examples.

EXHIBIT 3–1

INFORMATION ABOUT CALLS TERMINATING TO THE INTERCEPT SUBJECT

CALLING PARTY'S LINE INFORMATION	SERVICE TYPE	INTERCEPT SUBJECT'S LINE INFORMATION
• Directory Number (DN)	Plain Old Telephone Service (POTS)	• Directory Number (DN)
• Associated Directory Number • Line Equipment Identifier • Call Type/Bearer Capability • Service Profile Identifier (SPID)	Integrated Services Digital Network (ISDN)	• Associated Directory Number • Line Equipment Identifier • Call Type/Bearer Capability • Service Profile Identifier (SPID)
• Numbers used by the service provider switch to identify the PBX and the caller behind the PBX - Directory Number of the PBX - Station identifier of the calling party (if available)	Private Branch Exchange (PBX)	• Numbers used by the service provider switch to identify the PBX and the caller behind the PBX - Directory Number of the PBX - Station identifier of the called party (if available)
• Directory Number	Coin	• Directory Number
• Electronic Serial Number (ESN) • Mobile Identification Number (MIN)	Cellular	• Electronic Serial Number (ESN) • Mobile Identification Number (MIN)
• Personal Number/Directory Number • Terminal Equipment Identifier	Personal Communications Service (PCS)	• Personal Number/Directory Number • Terminal Equipment Identifier
• Directory Number • Other available items, for example, Automatic Numbering Identification (ANI)	Other Special and Proprietary Customer Premises Equipment (CPE) Interfaces (Non-POTS or Non-ISDN Signaling)	• Directory Number • Other available items, for example, Automatic Numbering Identification (ANI)

Line Information for Originating Calls. When the intercept subject originates a call, law enforcement requires access to information about the communications line used by the subject. The information available to describe a subject's line varies based on the type of communications service used by the intercept subject. Types of line identifiers include directory numbers (DN), mobile identification numbers (MIN), and personal numbers. Exhibit 3–2 presents several examples of information needed about the subject's line and required by law enforcement agencies when the intercept subject originates a call.

---

[2] The term "line" is used broadly to refer to the transmission path from a subscriber terminal to the network. This transmission path may be via a wireline or wireless medium (for example, copper wire, radio link).

EXHIBIT 3–2

INFORMATION ABOUT THE SUBJECT'S LINE WHEN THE SUBJECT ORIGINATES CALLS

SERVICE TYPE	LINE INFORMATION
Plain Old Telephone Service (POTS)	• Directory Number (DN)
Integrated Services Digital Network (ISDN)	• Directory Number Associated With the Call • Line Equipment Identifier • Call Type/Bearer Capability • Service Profile Identifier (SPID)
Private Branch Exchange (PBX)	• Numbers used by the service provider switch to identify the PBX and the caller behind the PBX: - Directory Number of the PBX - Originating station identifier
Coin	• Directory Number ·
Cellular	• Electronic Serial Number (ESN) • Mobile Identification Number (MIN)
Personal Communications Service (PCS)	• Personal Number/Directory Number • Terminal Equipment Identifier
Other Special and Proprietary Customer Premises Equipment (CPE) Interfaces (Non-POTS or Non-ISDN Signaling)	• Directory Number • Other available items, for example, Automatic Numbering Identification (ANI)

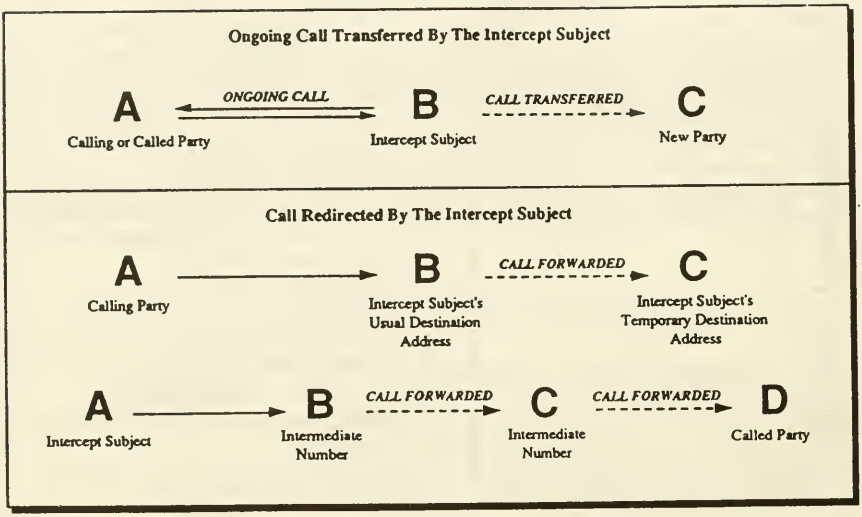
Dialing and Signaling Information. In addition to the subject's line information, law enforcement agencies require access to the dialing the signaling information generated by the subject for all calls originated by the intercept subject. Examples of dialing and signaling information include the following:

- All digits dialed by the subject and any signaling information used to establish or direct call flow
- Subsequent dialing information generated by the subject after cut-through
- The terminating number of the destination derived by the originating switch based on its interpretation of the subject's dialed digits or other call direction commands.

Redirection Numbers. Access to call setup information also includes redirection numbers when calls are forwarded or transferred using custom calling features. Law enforcement requires access to the forwarded-to number when the intercept subject transfers or forwards calls to another number. For a call terminating to the intercept subject, law enforcement agencies require access to any available redirection numbers when multiple forwards or transfers are involved in the call attempt. As an example, a call initiated by a calling party may be forwarded or transferred several times before reaching the intercept subject. Law enforcement requires the number of the calling party that originated the call, as well as any available intermediate numbers used to redirect the call. Exhibit 3–3 illustrates several all redirection scenarios.

EXHIBIT 3–3

CALL REDIRECTION SCENARIOS *



* A, B, C, and D may represent the same or different switches

Call Attempt Alerts. Law enforcement agencies require notification of all call attempts placed to or by the intercept subject. For example, in the case of a wireline intercept on a local loop, law enforcement generates a time stamp after detecting the local exchange carrier's (LEC) signaling for on-hook, ringing, and off-hook. However, local exchange carrier signaling protocols may change with emerging technologies. In future implementations, out-of-band signaling using signaling transfer points (STP) may replace in-band protocols currently used by law enforcement to detect call activity. Therefore, law enforcement agencies require some form of notification to provide a trigger for monitoring equipment.

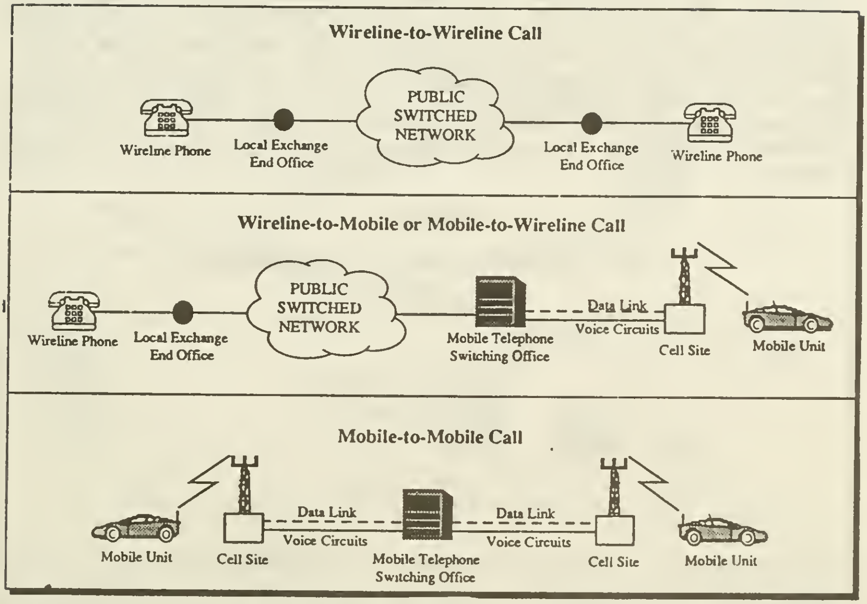
CALL CONTENT

Law enforcement agencies require access to call content for all calls originating from and terminating to the intercept subject's fixed or mobile number, terminal equipment, or other identifier. Access to call content is required regardless of the type of communications used in the call including cases when the communications between the intercept subject and other parties are sent and received over separate channels. The communications between the intercept subject and other parties may take place using wireline systems, wireless (mobile) systems, or a combination.

Service Arrangements. In a wireline-to-wireline call, both the calling and called parties use traditional wireline services. Examples of wireline services include coin, Plain Old Telephone Service (POTS), and Integrated Services Digital Network (ISDN). In a wireline-to-mobile or mobile-to-wireline call, one party uses a mobile communications service while the second party uses a wireline service. With mobile communications services, the service subscriber is able to communicate as he or she moves within a given region or area. Cellular and Personal Communications Service (PCS) are examples of mobile services. When both parties use a mobile service, the call is referred to as mobile to mobile. Exhibit 3–4 illustrates these types of call scenarios.

Exhibit 3–4

WIRELINE AND MOBILE COMMUNICATIONS EXAMPLES



In each of the scenarios presented in Exhibit 3–4, the call is switched by a specific entity before terminating to or after being originated by the intercept subject. Law enforcement agencies require access to call content regardless of the entities used to switch the calls. For example, in a mobile-to-mobile or wireline-to-mobile call, the call may be switched at a cell site, at a Mobile Telephone Switching Office (MTSO), or at a Personal Communications Switching Center (PCSC).

Custom Calling Features. Access to call content includes calls that have been redirected or have multiple call recipients. The obligation of service providers to provide access when custom calling features are invoked depends on whether the service provider that received the authorized intercept request maintains access to the call. When custom calling features are invoked, the service provider that received the authorized intercept request is required only to provide access to call content as long as the service provider maintains access to the communications. When an intercept subject uses a redirection feature that causes the loss of call access by the service provider, law enforcement requires notification of the identity of the new service provider now supporting the subject's communications. If the new service provider's identity is unavailable, law enforcement requires any information that will permit law enforcement agencies to determine the new service provider's identity. *In all cases, law enforcement agencies will coordinate delivery of communications in advance.*

MOBILITY

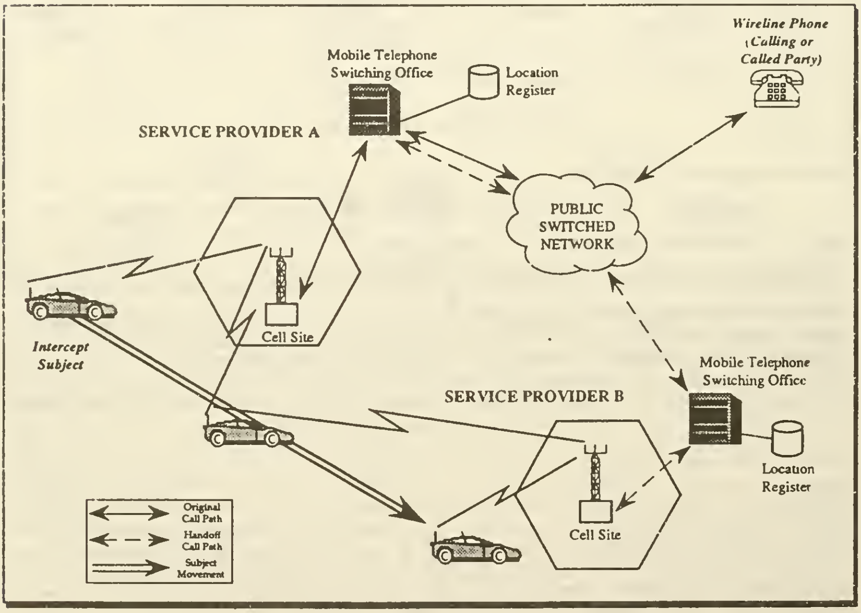
The requirement for lawful access to call content and call setup information applies equally to mobile telecommunications services. With mobile telecommunications services, a subscriber may move freely within predefined areas and communicate using portable units, terminals, or personal numbers. Law enforcement requires access to an intercept subject's communications throughout the service areas operated by the service provider that has been served with a lawful authorization to intercept. When an intercept subject travels into another service provider's area, law enforcement requires access to ongoing calls only if the service provider maintains access to the subject's communications. When access to the subject's call is not maintained, law enforcement requires the identity of the visited service provider or information that will permit agencies to determine the visited service provider's identity.

The following clarifications and examples focus on cellular communications, which is an existing and well understood technology. However, the requirements apply equally to other mobile communications services.

Handoffs. Law enforcement agencies require continuous access to all ongoing calls regardless of any handoffs that may occur, as long as the service provider retains access to the call. This includes cases where the intercept subject moves within a service provider's system or between service provider systems. Exhibit 3–5 illustrates the case when an intercept subject, using a cellular service, travels into another service provider's area during an active call. In this illustration, the Mobile Telephone Switching Office serving the end user maintains access to the call and continues to provide law enforcement with access to the intercept subject's communications.

EXHIBIT 3–5

A MOBILE INTERCEPT SUBJECT'S COMMUNICATIONS

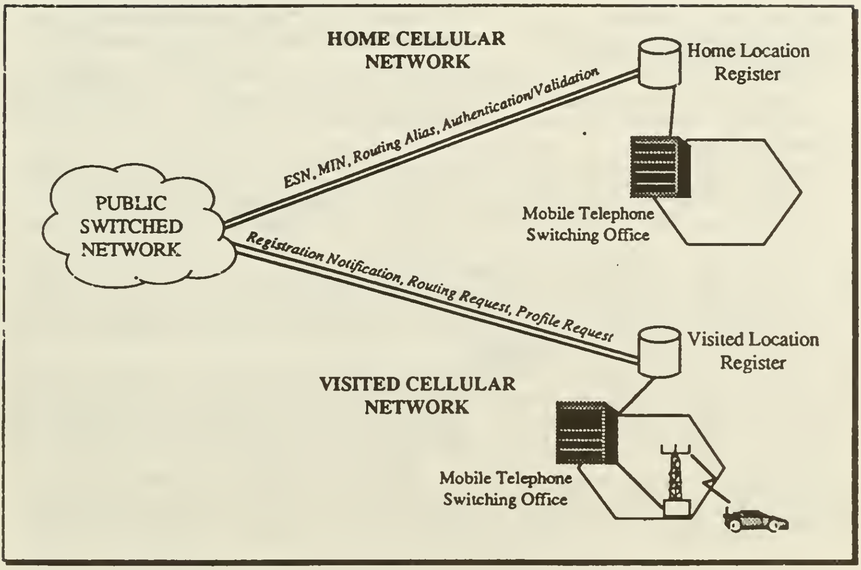


Roaming. The access requirement applies when the intercept subject uses roaming features. This requirement assumes that service providers supporting the subject's communications have received the appropriate lawful authorization from law enforcement and that delivery of the communications has been coordinated. Law enforcement is not asking for an automatic, seamless, nationwide intercept capability for subjects traveling across multiple service provider boundaries. A service provider's network may encompass local, regional, or interstate areas depending on the scope coverage offered by the service provider. However, when a service provider offers a nationwide service and lawful authorizations permit interception, law enforcement agencies require access to communications for an intercept subject roaming within that service provider's network.

Registration Information. Law enforcement agencies require access to information regarding the identity of service providers requesting visit registration authorization for an intercept subject. For cellular services, Exhibit 3–6 depicts the case when an intercept subject travels into a new service provider's area and requests service.

EXHIBIT 3–6

REGISTRATION INFORMATION EXCHANGE


HOME CELLULAR NETWORK
Home Location Register
ESN, MIN, Routing Alias, Authentication/Validation
PUBLIC SWITCHED NETWORK
Mobile Telephone Switching Office
Registration Notification, Routing Request, Profile Request
Visited Location Register
VISITED CELLULAR NETWORK
Mobile Telephone Switching Office

The exhibit illustrates that during registration, information is exchanged between the original service provider's location register and the visited location register. The original service provider is under an existing lawful authorization to provide access to the intercept subject's communications. In this example, law enforcement requires that the original service provider notify law enforcement of the new service provider's identity, or provide any other information that permits law enforcement agencies to determine the identity of the visited service provider.

Service Site Information. In certain situations and with appropriate lawful authorizations, law enforcement agencies may request the most accurate information available from the service provider's network elements regarding the site from which services are being provided to the intercept subject. For example, in a cellular system, service site information may include the cell site serving the intercept subject or the identity of the service provider supporting communications after a handoff.

REQUIREMENT 2 (REAL-TIME, FULL-TIME MONITORING)

Law enforcement agencies require a real-time, full-time monitoring capability for intercepts.

Real-time/Full-time Access. Law enforcement agencies require real-time access to an intercept subject's communications content and call setup information. The term "real-time" in Requirement 2 refers to monitoring that occurs as the intercepted communications take place, rather than the monitoring of a recording of the communications. In actuality, there is a small transmission delay from the moment intercepted communications occur to the moment the signals reach the monitoring equipment. Real-time monitoring of data communications may occur at any time between the sending of a data transmission by the originating terminal equipment and the receiving of the data transmission by the destination terminal equipment. Full-time monitoring refers to the ability to access and monitor all service activity associated with the intercept subject on a 24 hour-per-day basis.

REQUIREMENT 3 (TRANSMISSION)

Law enforcement agencies require service providers to transmit intercepted communications to a monitoring facility designated by the law enforcement agency.

Transmission of Intercepted Communications. Law enforcement agencies require the transmission of the intercept subject's call content and call setup information to a designated law enforcement monitoring facility. Access to intercept features is controlled by service providers. Law enforcement agencies will work with service providers in advance to arrange for delivery of intercepted communications to a monitoring location. Guidelines for the transmission of intercepted communications are:

- If call setup information and call content are separated, law enforcement agencies require service providers to ensure accurate association of call setup information with call content.
- Law enforcement agencies require service providers to be able to transmit the intercepted communications to a monitoring location without altering the call content or meaning (exclusive of any signal formats required for delivery to law enforcement).
- Law enforcement agencies require that the facilities and format for transmitting the intercepted communications to the monitoring location be standard or generally available (for example, leased line, switched connection, analog voice). The formats will be jointly agreed upon by law enforcement and service providers.
- If the service provider controls and/or provides coding, compression, encryption, or any other security technique on the intercepted communications, law enforcement agencies require the service provider to decode, decompress, or decrypt the intercepted communications or provide capabilities for decoding, decompressing, or decrypting the communications.
- Law enforcement agencies require that service providers use a minimum number of transmission facilities to deliver the intercepted communications to the monitoring facility (for example, today most intercepts for cellular communications in service areas with multiple MTSO's require a connection from each MTSO to the monitoring location for one intercept subject).
- As new technologies and services are developed, law enforcement agencies require that service providers have the ability to upgrade the delivery mechanism over time, allowing for phased changes in law enforcement collection systems.

REQUIREMENT 4 (TRANSPARENCY)

Law enforcement agencies require the intercept to be transparent to all parties except the investigative agency or agencies requesting the intercept and specific individuals involved in implementing the intercept capability. Law enforcement agencies require the implementation of safeguards to restrict access to intercept information.

Transparency of Interception. The intercept must remain transparent to all parties except for the monitoring agency and the electronic communications industry personnel involved in implementing the intercept. Law enforcement agencies require that the intercept remain transparent to the intercept subject, to all parties called by or calling the intercept subject, and to any other service subscribers not directly involved in communications with the intercept subject. At a minimum, the transparency of an intercept may be measured by the following attributes:

- Indications that an intercept is underway should not be discernible to the subject or other parties.
- If the implementation of an intercept occurs during an ongoing call, the intercept should not disrupt or interrupt the ongoing call (that is, no interruption or alteration of communications on active channels).
- If the implementation of an intercept causes changes in the operation of services and features, such changes should not be perceptible to the subject or other parties.
- If any noise is introduced by the implementation of an intercept, such noise should not be perceptible to the subject or other parties.

Safeguards for Intercept Access and Transparency. Service providers are not expected to ensure transparency beyond the capabilities of their own equipment.

There may be cases where the subject possesses sophisticated equipment to detect intercepts. To meet transparency requirements, the services provided to the intercept subject or any other subscriber should continue to comply with industry standards for transmission characteristics.

Law enforcement agencies also require that the service provider's operating procedures contain safeguards to preclude unauthorized or improper use of intercepts and to prevent a compromise of transparency. Example safeguards include:

- Restrictions on access to information about intercepts.
- Security mechanisms for activating and deactivating intercepts (for example, passwords).

- Physical security to limit access to systems supporting intercepts.
- Procedures to prevent subjects from being notified of service changes caused by the implementation of intercepts.
- Restriction of knowledge of intercepts to authorized service provider personnel (that is, personnel with a "need-to-know").

Service providers must immediately notify the appropriate law enforcement agency upon learning that intercept transparency was or may have been compromised.

REQUIREMENT 5 (VERIFICATION INFORMATION)

Law enforcement agencies require (1) information from the service provider to verify the association of the intercepted communications with the intercept subject, and (2) information on the services and features subscribed to by the intercept subject prior to intercept implementation and during the intercept.

Information Associating Communications With the Intercept Subject. Based on lawful inquiry, law enforcement agencies require information to verify the association of the intercepted communications with the network identifier (for example, directory number), terminal equipment identifier, and/or personal number of the intercept subject designated in the lawful authorization. Specifically, court authorities require law enforcement agencies to verify that the communications facility or service being intercepted corresponds to the subject or subjects identified in the lawful authorization. To accomplish the verification, law enforcement needs information, such as billing and caller identification-related information, from service providers. Service providers are not expected to provide information about the type of communications (for example, facsimile, electronic mail) or the customer premises equipment used by the intercept subject.

Service Profile Information. Law enforcement agencies also require that a subject's service profile information be made available upon a lawful inquiry. Service profile information may be requested before or during interception. Law enforcement agencies require notification from service providers of changes made to the intercept subject's service profile during an ongoing intercept regardless of how the changes are initiated. For example, a service profile change may be driven by a service order or directly initiated by the intercept subject.

REQUIREMENT 6 (SIMULTANEOUS INTERCEPTS)

Law enforcement agencies require service providers to make provisions for implementing a number of simultaneous intercepts. (Intercept demand will be estimated through a cooperative industry and law enforcement effort.)

Multiple, Simultaneous Intercepts. Law enforcement agencies need to be able to perform multiple, simultaneous intercepts within a given service provider's system, central office, area, etc. Law enforcement agencies and industry will need to work together to determine capacity ranges for use in developing intercept capabilities for a changing telecommunications environment. Law enforcement agencies require a service provider to support all requested lawfully authorized intercepts within its service area. As a result, law enforcement agencies require service providers to have reserve intercept capacities available to meet unexpected intercept demands that exceed projections. Law enforcement and industry should work together to achieve a "no held order" operating environment (that is, an environment where all intercept orders are fulfilled by service providers).

Interception of Multiple Calls and by Multiple Agencies. Law enforcement agencies need the ability to access and monitor all simultaneous calls originated or received by the intercept subject. In accordance with Requirement 4, multiple law enforcement agencies require the ability to monitor the same intercept subject while maintaining transparency.

REQUIREMENT 7 (EXPEDITIOUS ACCESS)

Law enforcement agencies require service providers to expeditiously provide access to the communications of the intercept subject.

Access Activation/Deactivation. Law enforcement agencies require each service provider to have defined or standardized procedures for activating and deactivating intercepts, and to provide access to the intercept subject's communications within 24 hours or less upon receipt of a lawful intercept request. Law enforcement agencies may also require expeditious access to appropriate technical resources or points of contact for assistance in activating the intercept or acquiring necessary service information (for example, service site information or service profile information).

BOSTON PUBLIC LIBRARY
3 9999 05983 093 3

Access Under Special Conditions. When special inside or outside plant construction is required to implement the intercept (for example, the construction of a leased line), law enforcement agencies require access to the intercept subject's communications within 5 business days or a period determined feasible by the service provider and law enforcement. In "emergency situations," law enforcement agencies require access to the intercept subject's communications within a few hours, and access to technical resources for assistance with the intercept. Law enforcement may elect to defer some requirements in certain exigent circumstances, thereby enabling a service provider to comply with an order to meet urgent investigative needs. Emergency situations are determined by law enforcement and apply to time-critical investigations, such as cases where rapid response is required to eliminate threats to life, property, or national security. Law enforcement will provide service providers with as much prior notification as possible. "Emergency" situations relate to electronic surveillance conducted pursuant to United States Code.[3]

REQUIREMENT 8 (RELIABILITY)

During the intercept period, law enforcement agencies require that the reliability of the services supporting the intercept at least equals the reliability of the communication services provided to the intercept subject.

Reliability of Intercept. Law enforcement agencies require that the reliability of the service supporting the intercept be at least equal to the reliability of the subject's service. Reliability refers to the probability that a system or product will perform in a satisfactory manner for a given period of time when used under specified operating conditions. Law enforcement agencies also require that service providers have the ability to detect and resolve problems with (1) the interception of call setup information and call content, and with (2) the transmission of the intercepted communications to the designated monitoring facility. Finally, law enforcement agencies require that service providers have plans for ensuring that system upgrades, software upgrades, and other network management procedures do not disrupt or terminate ongoing intercepts.

REQUIREMENT 9 (QUALITY)

Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the service providers.

Quality of Intercept. Law enforcement agencies require that the quality of the service supporting the intercept be at least equal to the quality of the subject's service. Quality of service in regard to the intercept refers to the quality specification of the communications channel or system used to transmit the intercepted communications. For example, quality of service may be measured based on signal to noise ratio, bit error rate, or any other parameter for transmission quality.

GLOSSARY

Access. The technical capability to interface with a communications facility, such as a communications line or switch, so that law enforcement can monitor and receive call setup information and call content.

Call. Any wire or electronic signaling information generated by a human or a computer acting as an agent for a human to set up a physical or virtual connection to transmit information to another or multiple users (humans and/or computer processes).

Call Content. The same as "contents," as defined in 18, U.S.C. 2510(8) and with respect to any electronic communication, includes any information concerning the substance, purport, or meaning of that communication.

Call Setup Information. When used with respect to any electronic communication, the information generated during the establishment of communications or transmission of a protocol data unit, such as a datagram, that identifies the origin and destination of the call. For voice communications, this information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted, or caused to be transmitted, by the intercept subject. It also includes incoming pulses, tones, or messages that identify the number of the originating instrument, device, or user. For data services, this information is typically the source (calling) address and destination (called) address contained in fields of the data unit, such as in the header of a frame or packet.

---

[3] 18, U.S.C. 2518(7); 18, U.S.C. 2518(11)(b); 18, U.S.C. 3125(a); 50, U.S.C. 1805(e)

Electronic Communications. The same as defined in Section 2510(12) of 18, U.S.C., any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic photo-electric, or photo-optical system, etc. As used herein, the term includes "wire communications," as defined in 18, U.S.C. 2510(1).

Electronic Surveillance. The statutory-based process and the associated technical capability and activities of law enforcement agencies related to the interception and monitoring of electronic communications.

Inside Plant Construction. With respect to wire and cable, any modification to the cable plant extending inward beyond the cable vault (for example, central office equipment, local area network management center), including the protectors and associated hardware. With respect to wireless networks, all fixed ground communications equipment that is permanently located inside buildings (for example, the equipment within the Mobile Telephone Switching Office of a cellular provider).

Intercept Subject. Person or persons identified in the lawful authorization and whose incoming and outgoing communications are to be intercepted and monitored.

Law Enforcement. Federal, state, and local law enforcement agencies.

Outside Plant Construction. Any modification to the physical plant, such as cables, poles, ducts, conduits, wire, fiber, repeaters, load coils, and other equipment located between central offices and other switching entities, or between the central office/switching entity and the customer.

Roaming. The ability of subscribers of mobile telecommunications services to place and receive calls when they are located outside their designated home serving area.

Service Provider. Any public, quasi-public, or private supplier of electronic communications services providing users the ability to send or receive electronic communications (for example, local and long distance carriers, competitive access providers, public data service providers, and cellular service providers).

Transmission. The act of transferring a sign, signal, writing, image, message, sound, data or other form of intelligence (information) from one location to another by a wire, radio, electromagnetic, photo-electronic or photo-optical system.

Transparency. The circumstances wherein the parties to a communication and unauthorized individuals (that is, individuals who are not involved in implementing and maintaining the intercept) are unaware of ongoing electronic surveillance. For example, when applied to telephone communications, transparency refers to the interception of communications in such a way that the user is unaware of the intercept, and that does not affect the way the telephone functions are used.

Verification. The process whereby law enforcement can adequately demonstrate to a judge or jury that the number or other identifier (for example, telephone number, electronic mail address) targeted for interception corresponds to the person or persons whose communications are being intercepted. Typically, law enforcement verifies the identity of the subscriber whose facility or service is being intercepted.

○

ISBN 0-16-047613-5
90000
9 780160 476136